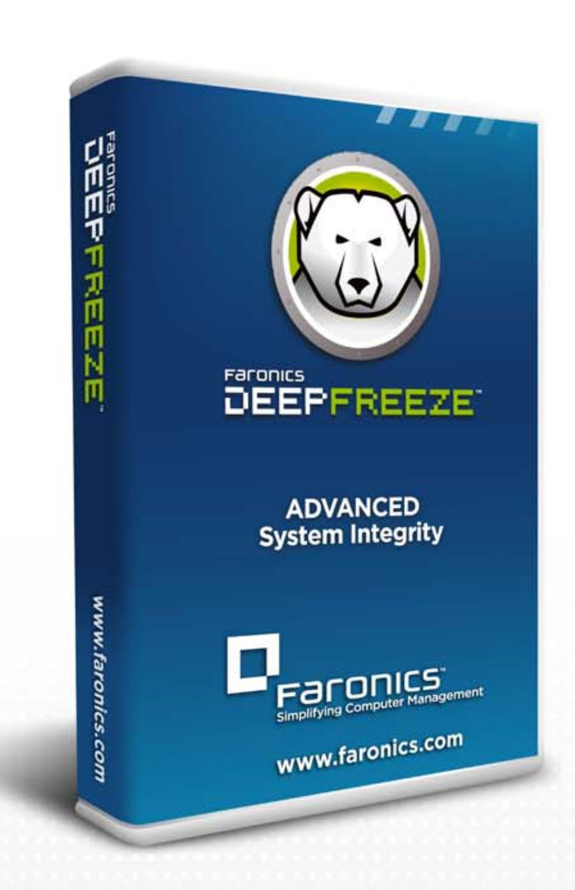




Deep Freeze

ADVANCED System Integrity

Guía del usuario

www.faronics.com








Modificado por última vez: junio de 2015



Contenidos









Prefacio

En este manual del usuario se explica cómo instalar, configurar y utilizar Deep Freeze Enterprise.

Temas



Información importante

Esta sección contiene información importante acerca de su producto de Faronics.

Acerca de Faronics

Faronics ofrece soluciones líderes en el mercado que ayudan a gestionar, simplificar y proteger entornos complejos de TI. Nuestros productos garantizan la total disponibilidad de los equipos y han mejorado significativamente la vida cotidiana de miles de profesionales de las tecnologías de la información. Las innovaciones tecnológicas de Faronics, con un claro enfoque en el mercado, están destinadas a instituciones educativas, centros de salud, bibliotecas, organizaciones gubernamentales y corporaciones.

Documentación del producto

La documentación de Deep Freeze Enterprise comprende los documentos siguientes:

- *Deep Freeze Enterprise Manual del usuario*: el documento que está leyendo en estos momentos. Este documento proporciona información sobre cómo usar el producto.
- *Deep Freeze Enterprise Notas de la versión*: este documento enumera las nuevas funciones y los problemas conocidos y cerrados.



Soporte Técnico

Hemos puesto todo nuestro empeño en diseñar un software que ofrezca una experiencia del usuario ágil y sin contratiempos. En caso de problemas, póngase en contacto con el equipo de soporte técnico.

Correo electrónico: support@faronics.com

Teléfono: 800-943-6422 o +1-604-637-3333

Horario: de 7.00 a 17.00 (Hora del Pacífico)

Información de contacto

- Web: www.faronics.com
- Correo electrónico: sales@faronics.com
- Teléfono: 800-943-6422 o +1-604-637-3333
- Fax: 800-943-6488 o +1-604-637-8188
- Horario: de 7.00 a 17.00 (Hora del Pacífico)

Dirección:

Faronics Technologies USA Inc.
100, W. San Fernando Street, Suite 465
San Jose, CA, 95113
USA

Faronics Corporation (oficina central)
609 Granville Street, Suite 1400
Vancouver, BC V7Y 1G5
Canada

Faronics Corporation (Europa)
Venture House, 2 Arlington Square, Downshire Way
Bracknell, RG12 1WA, England





Introducción



Deep Freeze protege los equipos que se han configurado para arrancar desde la unidad de disco duro. Configure el CMOS para arrancar desde la unidad de disco duro solamente. Es preciso proteger el CMOS con contraseña para evitar cambios no autorizados. Deep Freeze protege el registro de arranque principal (Master Boot Record, MBR) cuando el equipo está en modo Congelado.

Temas



Información general de Deep Freeze

Faronics Deep Freeze convierte la configuración de los equipos en indestructible para evitar daños y reducir el tiempo de inactividad. Una vez se haya instalado Deep Freeze en un equipo, cualquier cambio realizado en el equipo, independientemente de que sea fortuito o malicioso, nunca será permanente. Deep Freeze ofrece inmunidad inmediata ante muchos de los problemas que afectan a los equipos hoy en día: cambios inevitables de configuración, configuraciones erróneas accidentales en el sistema, actividad de software malicioso y degradación incidental del sistema.

Ahora es posible administrar Faronics Anti-Virus con Deep Freeze Enterprise (se necesita una licencia aparte para Faronics Anti-Virus). Faronics Anti-Virus ofrece protección contra amenazas de seguridad sin ralentizar los equipos debido a análisis lentos y a un uso excesivo de la memoria. Construido con tecnología de última generación, Faronics Anti-Virus le ofrece un software poderoso antivirus, antirootkit y antispyware todo en uno que protege los equipos de las complejas amenazas de malware actuales y permite una integración perfecta con Deep Freeze.

La integración de Deep Freeze con Faronics Anti-Virus garantiza que la protección esté actualizada de la forma más simple posible, y le proporciona capacidades de implementación y administración a través de la consola Deep Freeze Enterprise. Diseñados para trabajar juntos perfectamente, Faronics Anti-Virus se actualiza incluso cuando las estaciones de trabajo están en modo Congelado, lo que ofrece el sistema de protección más completo.



Requisitos del sistema

- Deep Freeze y Faronics Anti-Virus son compatibles con:
  - XP, Vista, Windows 7, Windows 8.1, Server 2003, 2008 y 2012
  - Windows Embedded 7 y 8
  - Deep Freeze requiere que se deje un 10% espacio libre en el disco duro.
  - Se admiten las versiones de Windows de 32 y 64 bits.
  - Windows XP (32 y 64 bits) debe tener instalado el Service Pack 2 o posterior.
- Faronics recomienda un mínimo de 256 MB de memoria en el sistema en los sistemas protegidos.
- El Administrador de configuración de Deep Freeze y la consola Enterprise son compatibles con:
  - XP, Vista, Windows 7, Windows 8.1, Server 2003, 2008 y 2012
  - Se admiten las versiones de 32 y 64 bits.
  - Windows XP (32 y 64 bits) debe tener instalado el Service Pack 2 o posterior.



Archivos de Deep Freeze Enterprise

Deep Freeze usa diferentes iconos de colores para representar sus componentes. Los archivos identificados con un icono rojo en general deben instalarse solamente en un equipo administrativo.

Icono	Definición
	Archivo de instalación de la consola Enterprise y el Administrador de configuración de Deep Freeze Enterprise.
	La aplicación Administrador de configuración se usa para crear archivos de programa de instalación personalizados y configurados previamente, y semillas (seeds) de estación de trabajo.
	La consola Enterprise se utiliza para implementar, controlar, administrar y mantener las instalaciones de Deep Freeze de forma centralizada.
	Se crea un archivo de instalación de estación de trabajo Deep Freeze en el Administrador de configuración y se implementa en las estaciones de trabajo de la empresa. Este archivo incluye la semilla de estación de trabajo. Si se instala el archivo de instalación de estación de trabajo Deep Freeze, no es necesario instalar la semilla de estación de trabajo por separado.
	Una semilla de estación de trabajo permite una comunicación optimizada entre la consola Enterprise y los equipos de una red. Cuando se instala la semilla de estación de trabajo en un equipo, el equipo se vuelve visible en la consola Enterprise. Una vez que un equipo es visible en la consola Enterprise, pueden realizarse diferentes acciones, como reiniciar, apagar y Wake-on-Lan, en el equipo de forma remota. Deep Freeze también puede instalarse de forma remota en un equipo visible para permitir acciones relacionadas con Deep Freeze en equipos remotos.



Instalación de Deep Freeze

En este capítulo se describe el proceso de instalación de Deep Freeze.

Temas



Proceso de instalación

Instalación del Administrador de configuración de Deep Freeze y la consola Enterprise

El Administrador de configuración ha sido diseñado para ser instalado únicamente en el equipo utilizado para administrar Deep Freeze. El Administrador de configuración se usa para crear archivos de instalación de Deep Freeze personalizados y semillas de estación de trabajo. La consola Deep Freeze Enterprise se instala automáticamente con el Administrador de configuración de Deep Freeze.



Si usa Deep Freeze 6.5 (o posterior), tiene la opción de actualizar de forma automática la consola Enterprise, el Administrador de configuración y los archivos de instalación/configuración de Deep Freeze (en la carpeta de programas de instalación) durante la instalación de Deep Freeze 8.1 (o posterior).

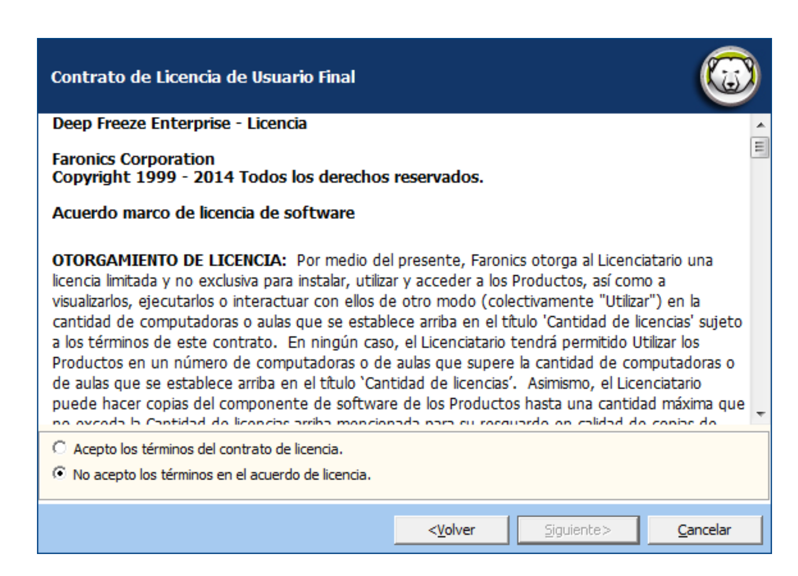
Siga los pasos descritos a continuación para instalar el Administrador de configuración:

1. Haga doble clic en el archivo *DFEnt.exe* para iniciar el proceso de instalación. Aparecerá la siguiente pantalla:

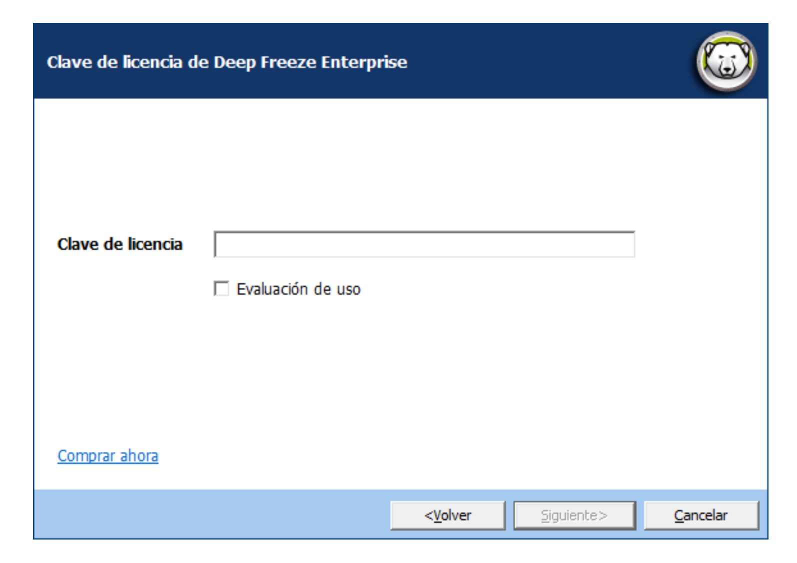


2. Haga clic en *Siguiente*. Lea y acepte el contrato de licencia. Haga clic en *Siguiente*.





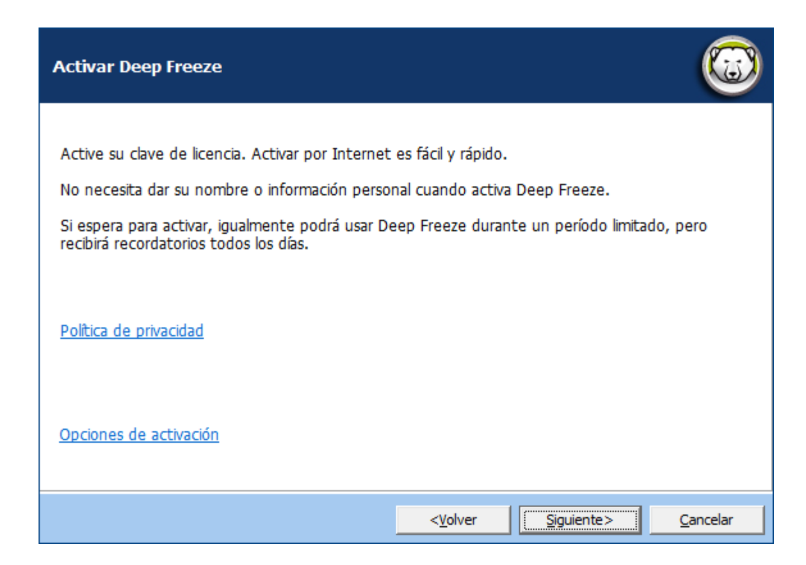
3. Introduzca la clave de licencia en el campo *Clave de licencia* o seleccione la casilla *Usar evaluación* para instalar en modo de evaluación. Haga clic en *Siguiente*.



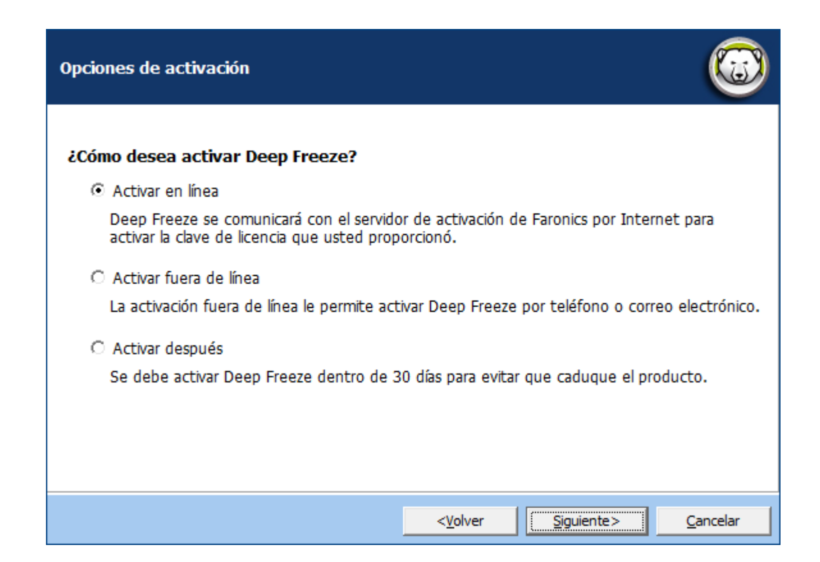
4. Introduzca la clave de licencia en el campo *Clave de licencia* o seleccione la casilla *Usar evaluación* para instalar en modo de evaluación. Haga clic en *Siguiente*.

5. Haga clic en *Siguiente* para ver las opciones de activación. Vuelva a hacer clic en *Siguiente* para activar la licencia de Deep Freeze a través de Internet. El equipo debe estar conectado a Internet para poder realizar la activación en línea. La licencia de Deep Freeze se debe activar dentro de los 30 días siguientes a la instalación; de lo contrario, recibirá recordatorios constantes para activar el producto. Durante la activación, Faronics autenticará la licencia de Deep Freeze.





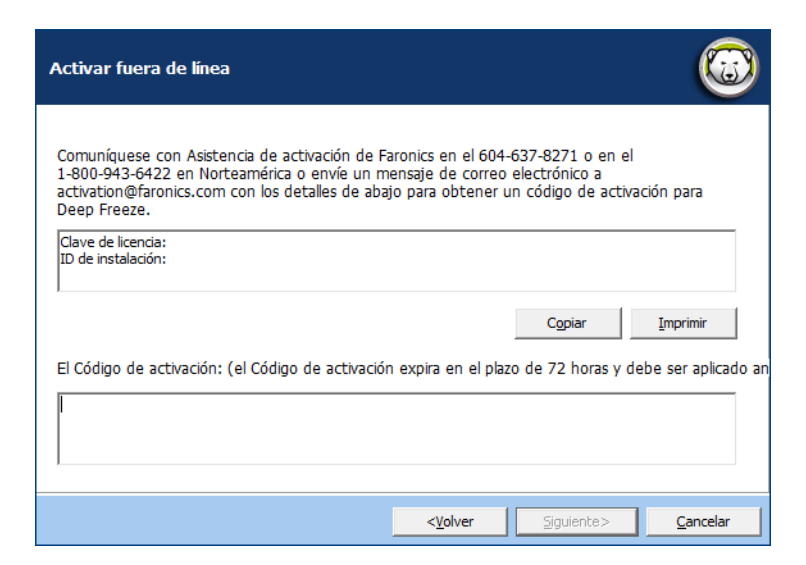
6. Como alternativa, haga clic en *Opciones de activación*. Hay tres opciones disponibles:

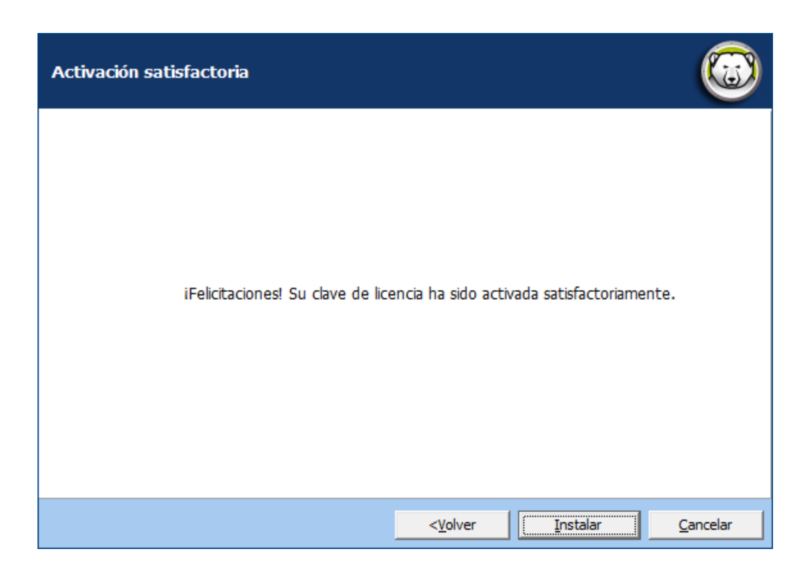


- Seleccione *Activar en línea* para activar la licencia de Deep Freeze en línea. Esta opción es igual que la del paso 4. Haga clic en *Siguiente* después de seleccionar esta opción. Deep Freeze se activará en línea al hacer clic en *Siguiente*.
- Seleccione *Activar sin conexión*. Esta opción permite realizar la activación por teléfono o correo electrónico. Haga clic en *Siguiente* después de activar. Aparecerá la pantalla Activar sin conexión.
- Seleccione *Activar más tarde*. Esta opción permite realizar la activación en otro momento.

7. Si ha seleccionado Activar sin conexión, envíe la clave de licencia y el Id. de instalación al Servicio de activación de Faronics por teléfono o correo electrónico. Una vez que reciba el código de activación de Faronics, introdúzcalo en el campo *Código de activación* y haga clic en *Siguiente*. Ahora la licencia de Deep Freeze está activada.

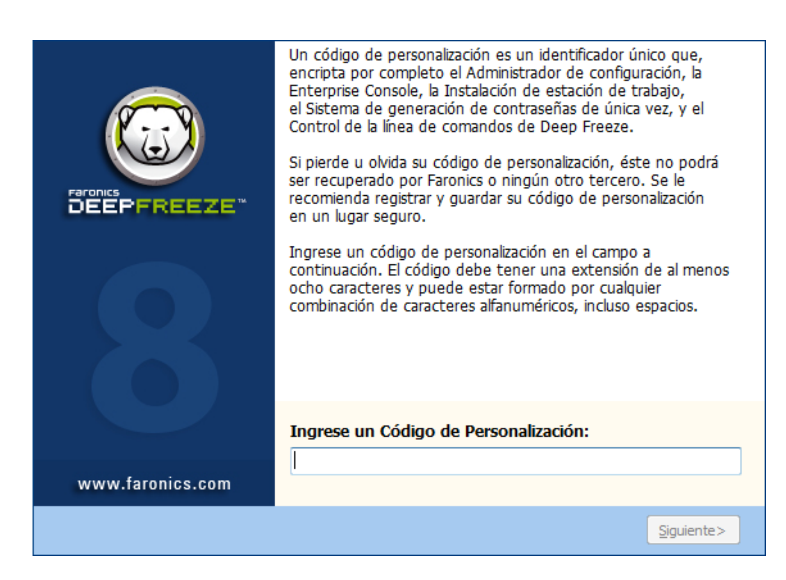






8. Una vez que haya finalizado el proceso de instalación, aparecerá la pantalla *Código de personalización*.





9. Especifique el *Código de personalización* y haga clic en *Siguiente*. El *código de personalización* debe tener un mínimo de ocho caracteres. La instalación se ha completado.



Código de personalización

El código de personalización es un identificador único que cifra el Administrador de configuración, la consola Enterprise, los archivos de instalación del equipo, el sistema de generación de contraseñas de un solo uso y el control de la línea de comandos de Deep Freeze. Este código no es una contraseña que pueda utilizarse para acceder a Deep Freeze.

El código de personalización evita que los administradores no autorizados puedan acceder a un equipo o controlarlo. Si varios administradores de Deep Freeze controlan el mismo grupo de equipos, es preciso que todos utilicen el mismo código de personalización.



Es preciso anotar y guardar el código de personalización a buen recaudo, ya que Faronics no puede recuperar los códigos de personalización perdidos u olvidados.

Reinicialización del código de personalización

Si otro administrador desea crear archivos de instalación con el mismo Administrador de configuración mediante un código de personalización diferente, siga los pasos descritos a continuación:

1. Ejecute *DFInit.exe*.
2. Se restablecerá el código de personalización existente para el Administrador de configuración y la consola Enterprise.
3. Introduzca un nuevo código de personalización.
4. Haga clic en *Aceptar* para activar el nuevo código de personalización.

Modo de actualización

El modo de actualización puede utilizarse para crear de forma automática versiones actualizadas de archivos de Deep Freeze Enterprise existentes mediante la ejecución de un comando de *actualización* especial. Este comando realiza dos tareas:

- Actualiza las versiones previas de la consola Deep Freeze Enterprise y el Administrador de configuración de Deep Freeze. (Ubicadas en *Faronics* > *Deep Freeze 7 Enterprise*.)
- Actualiza todos los archivos creados por el usuario guardados en la carpeta *Faronics* > *Deep Freeze 7 Enterprise* > *Install Programs*.

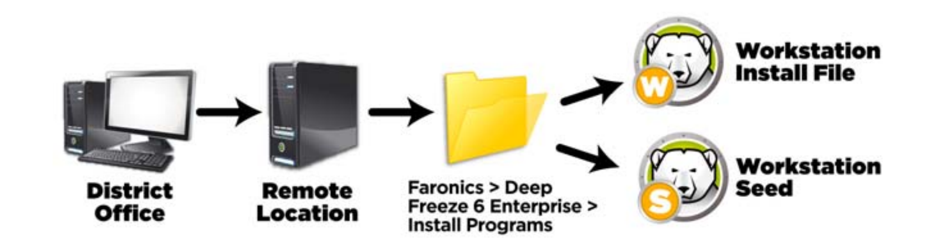
La ventaja de estas actualizaciones es que es posible actualizar varios archivos a la versión más reciente sin perder sus datos de configuración (creados con una versión anterior de Deep Freeze Enterprise).

El comando actualiza automáticamente los archivos creados por un administrador (*.exe*, *.rdx*) que están presentes en el directorio *Faronics* > *Deep Freeze 7 Enterprise* > *Install Programs*, incluidos los siguientes subdirectorios:

- *Archivos de instalación de estación de trabajo*
- *Archivos de semilla de estación de trabajo*



En el siguiente ejemplo, la oficina del distrito ha recibido una nueva versión del Administrador de configuración de Deep Freeze y puede actualizar de forma automática cualquier archivo de instalación de estación de trabajo Deep Freeze y semilla de estación de trabajo en una ubicación remota.



El comando de actualización no requiere una contraseña, pero sí un código de personalización. Utilice la siguiente sintaxis de comandos:

```
\RutaAArchivo\DFEnt.exe /update=”código de personalización”
c:\dfupdate.log
```

- *RutaAArchivo* debe sustituirse por la ruta actual al archivo de instalación (*DFEnt.exe*)
- *DFEnt.exe* sustitúyalo por el nombre real del archivo de instalación (puede ser diferente si se ha descargado)
- Es preciso escribir el código de personalización entre comillas si contiene algún espacio.
- El código de personalización debe coincidir con el código de personalización de los archivos de instalación antiguos.

El archivo de registro proporciona información detallada sobre los archivos que se han actualizado.

El proceso de actualización puede llevar unos minutos.

El modo de actualización no actualiza la versión de Deep Freeze existente en los equipos. Los equipos deben actualizarse con la consola Enterprise.



Contraseña de un solo uso

El sistema de generación de contraseñas de un solo uso permite generar contraseñas temporales para Deep Freeze que caducan a la medianoche del día en que se crearon.

Se puede acceder al cuadro de diálogo de contraseñas de un solo uso a través de

- *Herramientas>Contraseñas de un solo uso* en la consola Enterprise. Para obtener más información, consulte *Uso de la consola Deep Freeze Enterprise*.
- *Archivo>Contraseñas de un solo uso* en el Administrador de configuración. Para obtener más información, consulte *Utilización del Administrador de configuración de Deep Freeze*.

Una contraseña de un solo uso (OTP, por sus siglas en inglés) puede ser útil si, por ejemplo, no se recuerda una contraseña de Deep Freeze o si se ha creado un archivo de configuración sin una contraseña definida. Una contraseña de un solo uso también puede ser útil para proporcionar acceso a un equipo a un usuario que realice tareas de mantenimiento sin que sea necesario revelarle la contraseña permanente de Deep Freeze.

Siga los pasos descritos a continuación para crear una contraseña de un solo uso:

1. Seleccione *Contraseña válida para un solo uso* o *Contraseña válida para varios usos*. Todas las contraseñas de un solo uso caducarán a medianoche el día en que se crearon, independientemente del tipo que sean.
2. Introduzca el token de contraseña de un solo uso en el equipo correspondiente en el campo *Token*. El token de OTP para el equipo está ubicado en el cuadro de diálogo de inicio de sesión, como se muestra a continuación.



3. Haga clic en *Generar*.



La interfaz de línea de comandos de Deep Freeze no admite las contraseñas de un solo uso.





Utilización del Administrador de configuración de Deep Freeze

Temas



Acceso al Administrador de configuración

Seleccione la siguiente ruta en el menú Inicio para abrir el Administrador de configuración:

Inicio > Todos los programas > Faronics > Deep Freeze Enterprise 7 > Deep Freeze Administrator.

El Administrador de configuración dispone de varias fichas para configurar contraseñas: Unidades congeladas, Tareas de estación de trabajo, Actualizaciones de Windows, Archivos por lotes y Opciones avanzadas. Una vez se hayan configurado los ajustes, se podrá crear un archivo de instalación de estación de trabajo. El archivo de instalación de estación de trabajo puede instalarse en los equipos que deben protegerse con Deep Freeze. También se puede acceder al Administrador de Deep Freeze desde la consola Deep Freeze.

Barra de herramientas y menús

Barra de herramientas

La barra de herramientas está disponible en la parte superior de cada ficha del Administrador de configuración.

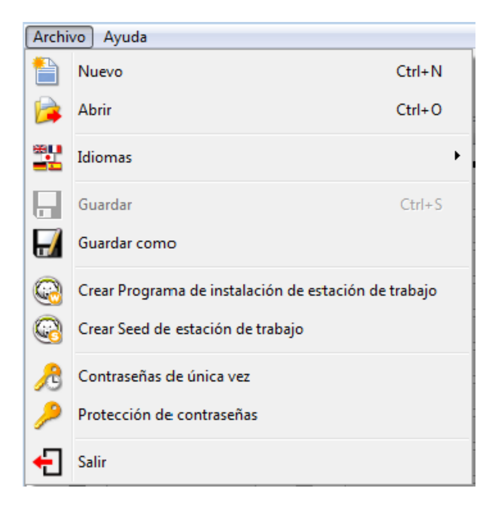


Icono	Función
Nuevo	Borra todos los ajustes de configuración existentes. Se abre con los ajustes de configuración predeterminados.
Abrir	Abra cualquier archivo de instalación de estación de trabajo, archivo de semilla de estación de trabajo o archivo .rdx guardado.
Guardar	Guarde un archivo de instalación de estación de trabajo, archivo de semilla de estación de trabajo o archivo .rdx. El nombre y la ruta del archivo se mostrarán en la parte inferior del Administrador de configuración en la sección de estado.
Guardar como	Guarde los ajustes de configuración como un archivo .rdx.
Ayuda	Acceda al archivo de Ayuda de Deep Freeze.
Crear	*Crear archivo de instalación de estación de trabajo* crea un instalador personalizado para la instalación en estaciones de trabajo. Las estaciones de trabajo pueden gestionarse desde la consola Deep Freeze Enterprise. *Crear archivo de semilla de estación de trabajo* crea una semilla que permite a la consola Deep Freeze comunicarse con las estaciones de trabajo a través de la red. Una vez se haya instalado la semilla en las estaciones de trabajo, se podrá implementar de forma remota el archivo de instalación de trabajo Deep Freeze.



Menú Archivo

El menú *Archivo* incluye las mismas opciones que la barra de herramientas y también permite seleccionar un idioma y la opción *Protección con contraseña*.



Protección con contraseña

La protección con contraseña ofrece un nivel de seguridad adicional para el administrador.

Para proteger con contraseña el acceso al Administrador de configuración, siga estos pasos:

1. Abra el menú *Archivo* y seleccione *Protección con contraseña*.
2. Active la casilla de verificación *Proteger con contraseña*.
3. Introduzca la contraseña y confírmela.
4. Haga clic en *Aceptar* para establecer la contraseña o en *Cancelar* para salir del cuadro de diálogo sin establecer una contraseña.





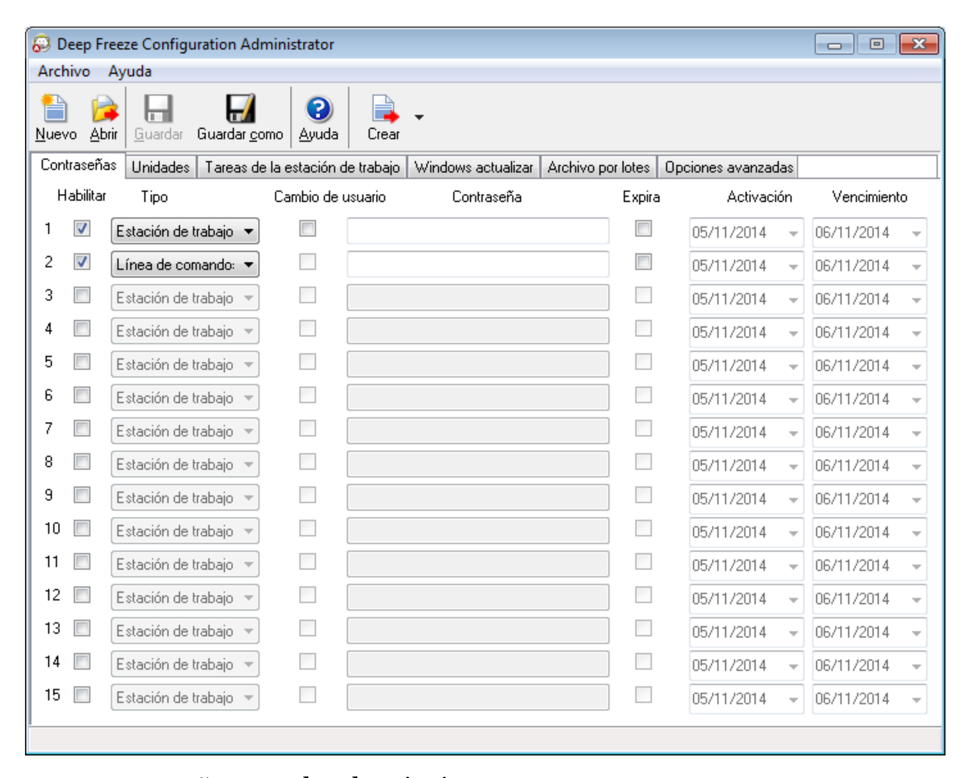


Guarde la contraseña en un lugar seguro. Si se pierde la contraseña, no podrá recuperarla. Tendrá que volver a instalar Deep Freeze.



Ficha Contraseñas

Deep Freeze Enterprise permite al administrador elegir hasta 15 contraseñas fijas.



Para crear una contraseña, complete los siguientes pasos:

1. Seleccione *Habilitar* en la fila apropiada.
2. En la lista desplegable *Tipo* seleccione el tipo de contraseña que desee. Estas son las opciones disponibles:
   - *Estación de trabajo*: contraseña que se debe introducir en la pantalla *Pantalla de inicio de sesión* de la estación de trabajo.
   - *Línea de comandos*: contraseña que se debe introducir para utilizar los controles de la línea de comandos. Para poder utilizar la herramienta de control de la línea de comandos (*DFC.exe*) es preciso definir una contraseña para la línea de comandos.
3. Opcional: también puede activar la casilla de verificación *Permitir cambio* para permitir al usuario cambiar la contraseña en el equipo.
4. Introduzca la contraseña.



La contraseña introducida en el campo *Contraseña* es visible.

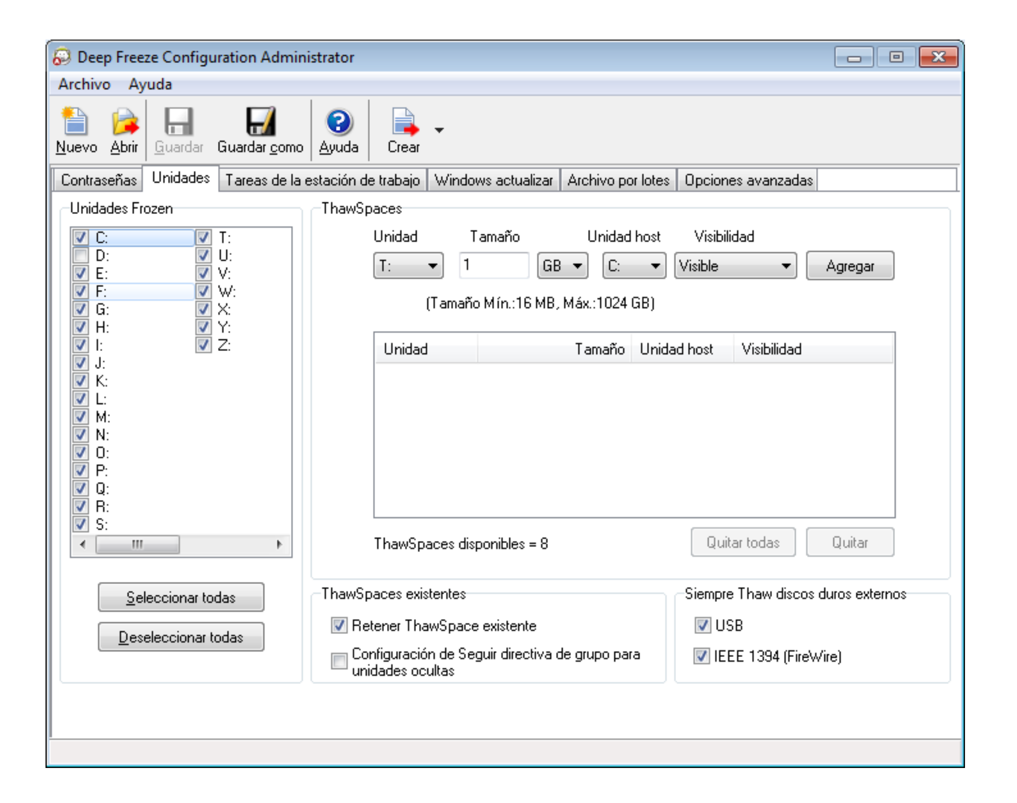
No utilice la misma contraseña para la línea de comandos y la interfaz gráfica de usuario.

5. Para configurar una contraseña que se active y caduque en unas fechas específicas, seleccione la casilla de verificación *Tiempo de espera* y utilice los cuadros de calendario para especificar una *Fecha de activación* y una *Fecha de caducidad*.



Ficha Unidades

La ficha Unidades permite especificar las unidades Congeladas (protegidas por Deep Freeze) o Descongeladas (no protegidas). También puede crear un ThawSpace, una partición virtual alojada en una unidad congelada o descongelada donde es posible guardar datos de forma permanente sin que Deep Freeze los elimine durante un reinicio.



Unidades congeladas

Todas las unidades están en modo Congelado de forma predeterminada. Para cambiar una unidad al modo Descongelado, desactive la casilla correspondiente a esa unidad.

Si bien solo es posible congelar las unidades locales (particiones o unidades físicas), se muestran todas las letras de unidades porque el archivo de instalación preconfigurado puede instalarse en varios equipos con distintas configuraciones de hardware y software.

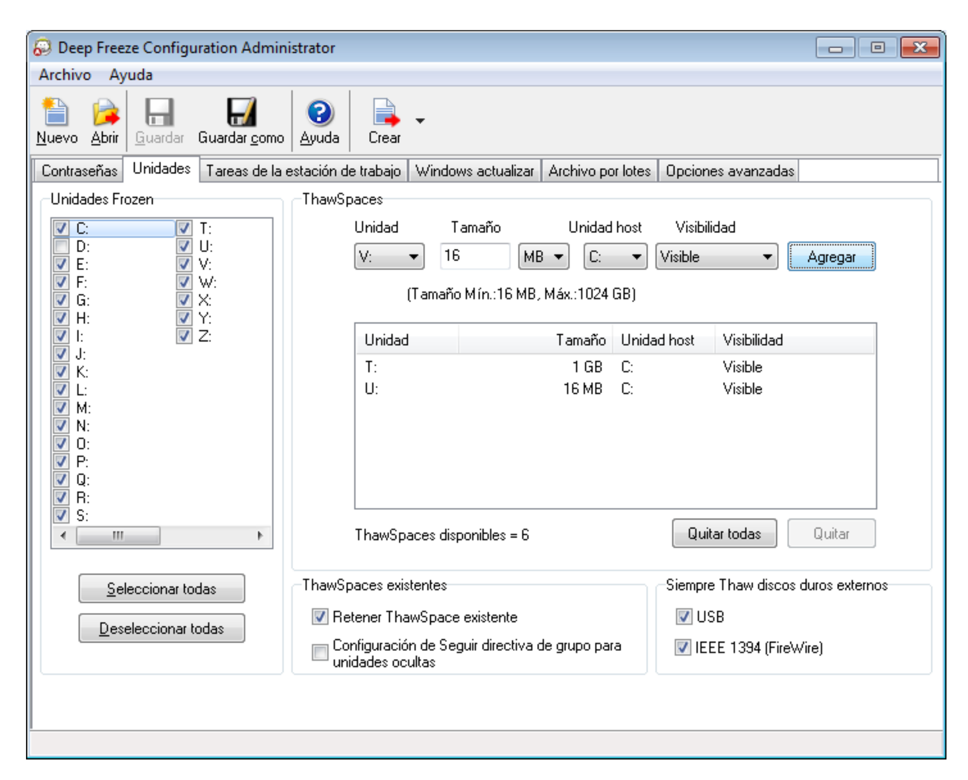
Ejemplo:

En la pantalla que se muestra arriba, *D:* no está seleccionada en la lista de unidades congeladas. Por consiguiente, todas las unidades, excepto *D:* están en modo Congelado.



ThawSpace

ThawSpace es una partición virtual que puede utilizarse para almacenar programas, guardar archivos o realizar cambios permanentes. Todos los archivos almacenados en el ThawSpace se conservarán después de un reinicio, aunque el equipo esté en modo Congelado. Es posible crear un ThawSpace en una unidad configurada como Congelada o Descongelada.



Para crear uno o varios ThawSpaces con el Administrador de configuración, siga los pasos descritos a continuación:

1. Seleccione la *Letra de unidad*. La letra predeterminada es *T:*. Sin embargo, puede cambiarla por cualquier otra letra disponible. La siguiente letra disponible se usa de forma automática si la letra de unidad seleccionada ya existe en un equipo.
   - Tras seleccionar una *Letra de unidad* para crear un ThawSpace, esta se eliminará de la lista desplegable.
   - Si se elimina el ThawSpace, la *Letra de unidad* correspondiente volverá a aparecer en la lista desplegable.
   - La *Letra de unidad* no puede ser la misma que la de la *Unidad de host*.



2. Introduzca el *Tamaño* del ThawSpace. El tamaño máximo es 1024 GB y el tamaño mínimo es 16 MB.
   - Si el equipo no tiene espacio suficiente para acomodar el tamaño seleccionado del ThawSpace, el tamaño del ThawSpace se reajustará a la baja para garantizar el correcto funcionamiento del equipo.
   - Si selecciona un tamaño inferior a 16 MB, el ThawSpace se establecerá automáticamente en 16 MB.
   - Si selecciona un tamaño superior a 1024 GB (1 TB), el ThawSpace se establecerá automáticamente en 1024 GB (1 TB).
3. Seleccione la unidad de almacenamiento del ThawSpace en *MB* o *GB*.
4. Seleccione la *Unidad de host*.
   - La *Unidad de host* es la unidad donde se creará el ThawSpace.
   - El almacenamiento necesario para el ThawSpace se obtiene del almacenamiento total disponible en la *Unidad de host*.
5. Seleccione *Visible* u *Oculto* en la lista desplegable *Visibilidad*.
   - Si selecciona *Visible*, la unidad se mostrará en el Explorador de Windows.
   - Si selecciona *Oculto*, no se mostrará en el Explorador de Windows.
   - Para acceder a la unidad oculta, escriba la letra de unidad en *Inicio>Ejecutar*.
6. Haga clic en *Agregar* para agregar el ThawSpace.

Eliminar un ThawSpace

Para eliminar un ThawSpace, selecciónelo y haga clic en *Quitar*. Se eliminará el ThawSpace y la letra de unidad volverá a aparecer en la lista desplegable *Letra de unidad*. Haga clic en *Quitar todo* para eliminar todos los ThawSpaces.



Antes de eliminar un ThawSpace, elimine cualquier redirección de perfil o enlace simbólico.

Al eliminar un ThawSpace, también se eliminarán los datos almacenados en él.

Los ThawSpaces no están protegidos por Deep Freeze. Implemente opciones de protección de datos adicionales, como procedimientos de copia de seguridad o antivirus.

Ejemplo:

En la pantalla que se muestra arriba, se creó un *ThawSpace* de 16 MB en la *Unidad de host* C: y el ThawSpace se designó con la letra de unidad *T:*. El ThawSpace *T:* está configurado como *Visible* y es posible acceder a él a través del Explorador de Windows.



Se recomienda asignar letras del final del abecedario (X, Y, Z) para evitar la reasignación automática cuando se desconecte una unidad extraíble.



ThawSpace existente

La casilla de verificación *Conservar los ThawSpaces existentes* está activada de forma predeterminada para evitar que se eliminen los ThawSpaces creados en instalaciones previas.

En las desinstalaciones atendidas, siempre se mostrará un cuadro de diálogo para pedirle si es preciso conservar o eliminar los ThawSpaces, independientemente de que se haya seleccionado la casilla de verificación *Conservar los ThawSpaces existentes*. Esta opción no se mostrará si la desinstalación se realiza a través de la consola Enterprise.

Configuración de Seguir directiva de grupo para unidades ocultas permite que la configuración de la directiva de grupo para unidades ocultas no entre en conflicto con la configuración de Deep Freeze para unidades ocultas.

La configuración de unidades ocultas para directivas de grupo es específica del usuario. La configuración de unidades ocultas para Deep Freeze es global si la opción *Configuración de Seguir directiva de grupo para unidades ocultas* está deshabilitada.



Si no hay directivas de grupo para unidades ocultas, se recomienda deshabilitar esta opción.

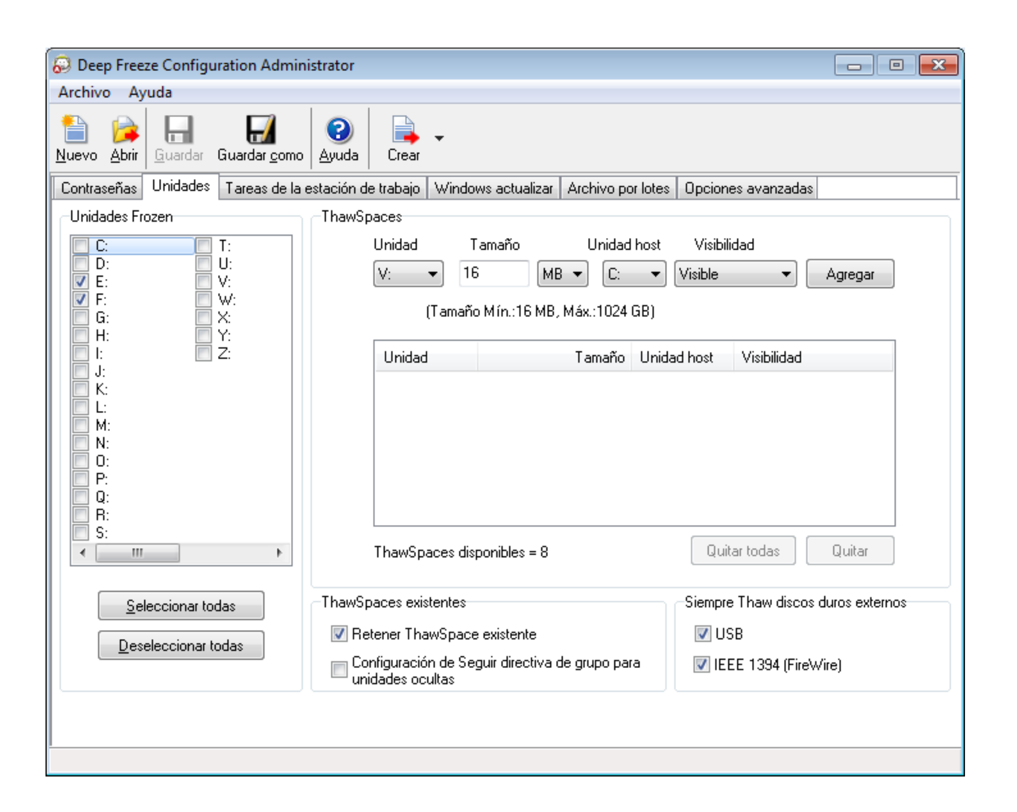
Descongelar siempre unidades de disco duro externas

El panel *Descongelar siempre unidades de disco duro externas* tiene dos casillas de verificación, *USB* e *IEEE 1394 (FireWire)* y ambas casillas están activadas de forma predeterminada. Esto garantiza que las unidades de disco duro USB o IEEE 1394 (FireWire) estén siempre en modo Descongelado.

Si las casillas de verificación de unidades de disco duro externas USB y/o IEEE 1394 (FireWire) están desactivadas, la unidad estará en modo *Congelado* o *Descongelado* en función de la letra en la que cada unidad se encuentre montada en la sección Unidades congeladas.

Las unidades de red y las unidades de medios extraíbles (disquetes, memorias externas, CD-RW, etc.) no se ven afectadas por Deep Freeze y, por lo tanto, no pueden ponerse en modo Congelado.





Ejemplo:

En la pantalla que se muestra arriba, las unidades *E:* y *F:* están seleccionadas en el panel *Unidades congeladas*.

Asumamos que *E:* corresponde a una unidad de disco duro USB y *F:* a una unidad de disco duro IEEE 1394 (FireWire).

Si se activan las casillas de verificación *USB* e *IEEE 1394 (FireWire)* en el panel *Descongelar siempre unidades de disco duro externas*, las unidades de disco duro externas estarían en estado *Descongelado*.

Si se activa la casilla de verificación USB y se desactiva la casilla de verificación *IEEE 1394 (FireWire)*. En este ejemplo, la unidad *USB* (*D:*) estaría en modo Descongelado y la unidad *IEEE 1394 (FireWire)* (*F:*) en modo Congelado.

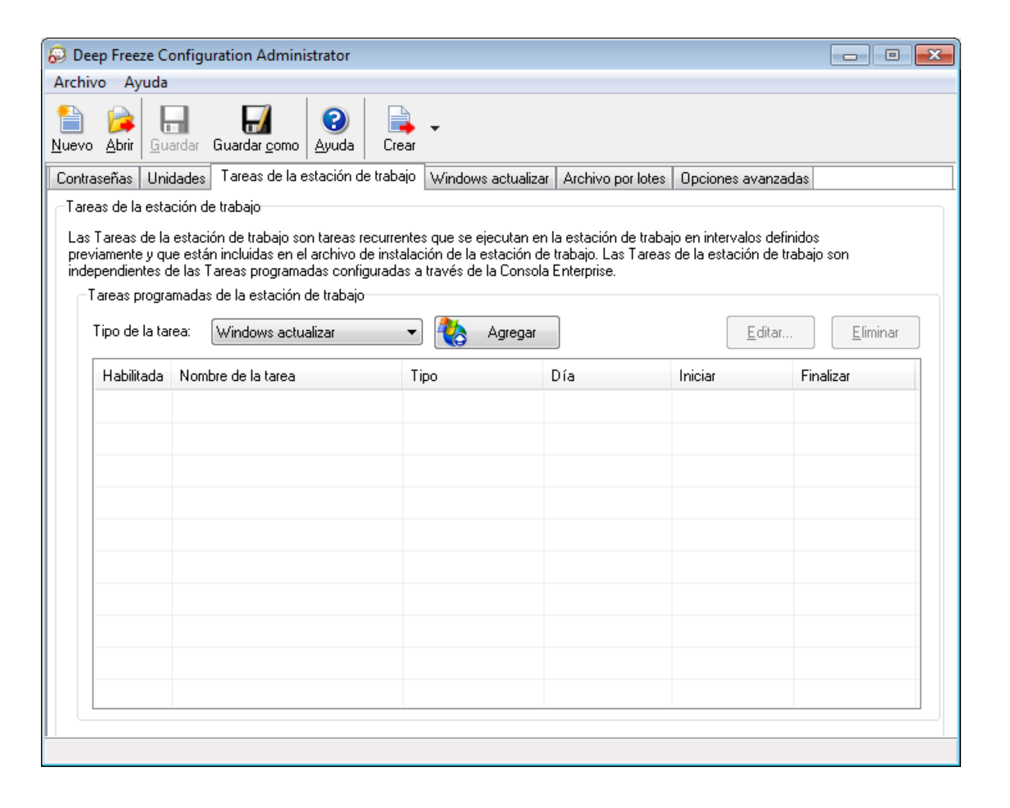


Ficha Tareas de estación de trabajo

La ficha Tareas de estación de trabajo le permite programar diversas tareas que se ejecutan en la estación de trabajo. Las Tareas de estación de trabajo residen en la estación de trabajo y se ejecutarán aunque las estaciones de trabajo pierden su conectividad de red o no puedan comunicarse con la consola Deep Freeze. Las Tareas de estación de trabajo son parte del archivo de instalación de estación de trabajo o archivo de configuración de Deep Freeze (.rdx). Están disponibles las tareas siguientes:

- *Actualización de Windows*: permite programar actualizaciones de Windows. Puede configurar ajustes adicionales en la ficha Actualización de Windows.
- *Reiniciar*: reinicia las estaciones de trabajo periódicamente para restablecer su configuración original o para borrar datos no deseados.
- *Apagar*: apaga las estaciones de trabajo cada día a una hora especificada para ahorrar energía.
- *Tiempo de inactividad*: apaga o reinicia las estaciones de trabajo si están inactivas durante un periodo de tiempo especificado.
- *Archivo por lotes*: ejecuta un archivo por lotes en las estaciones de trabajo seleccionadas. Puede configurar ajustes adicionales en la ficha Archivo por lotes.
- *Periodo de descongelación*: reinicia las estaciones de trabajo como descongeladas durante un periodo de tiempo especificado para realizar instalaciones de software manuales, instalaciones de software automatizadas con herramientas de terceros u otros cambios de configuración permanentes.

Cada tarea se explica en detalle en las secciones siguientes.







Tareas de estación de trabajo vs. Tareas programadas: Si la comunicación entre la consola Enterprise y el equipo de destino falla, las tareas de estación de trabajo seguirán ejecutándose puesto que existen en el equipo de destino.

Las tareas programadas a través del Asistente para tareas programadas de la consola Deep Freeze Enterprise existen en la consola Enterprise y no en los equipos de destino. Por consiguientes, para que las tareas programadas se ejecuten, se requiere una conectividad permanente entre la consola Enterprise y el equipo de destino. Para obtener más información, consulte la sección *Programación de tareas de Deep Freeze*.



Las tareas creadas en la ficha Tareas de estación de trabajo no pueden solaparse. Si una nueva tarea se solapa con otra existente, se mostrará un mensaje.



Se puede mostrar un mensaje al usuario durante un máximo de 5 minutos. Debe haber un lapso de tiempo de al menos 5 minutos entre dos tareas.



Las tareas de estación de trabajo solo se activan cuando Deep Freeze está en modo Congelado.

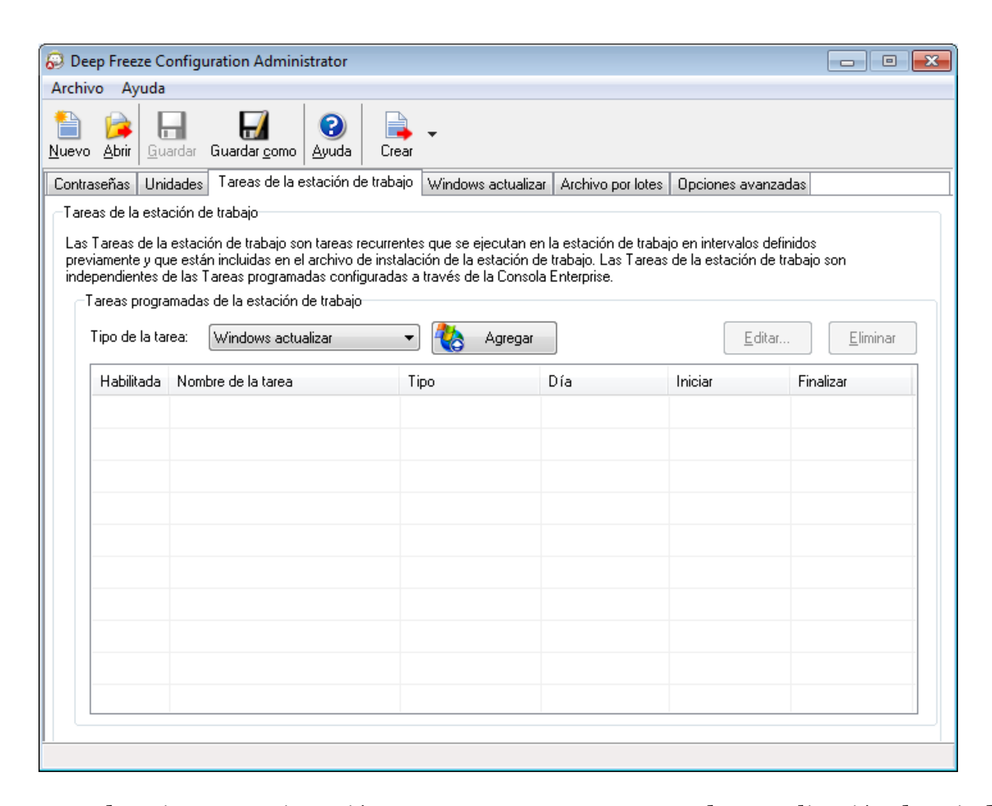
Actualización de Windows

Las tareas de actualización de Windows permiten descargar actualizaciones de Windows en la estación de trabajo. Las actualizaciones de Windows pueden descargarse aunque la estación de trabajo esté en modo Congelado. Una tarea de actualización de Windows tiene una hora de inicio y una hora de finalización. Una vez descargadas las actualizaciones de Windows, la estación de trabajo se reiniciará en modo Descongelado para aplicarlas.



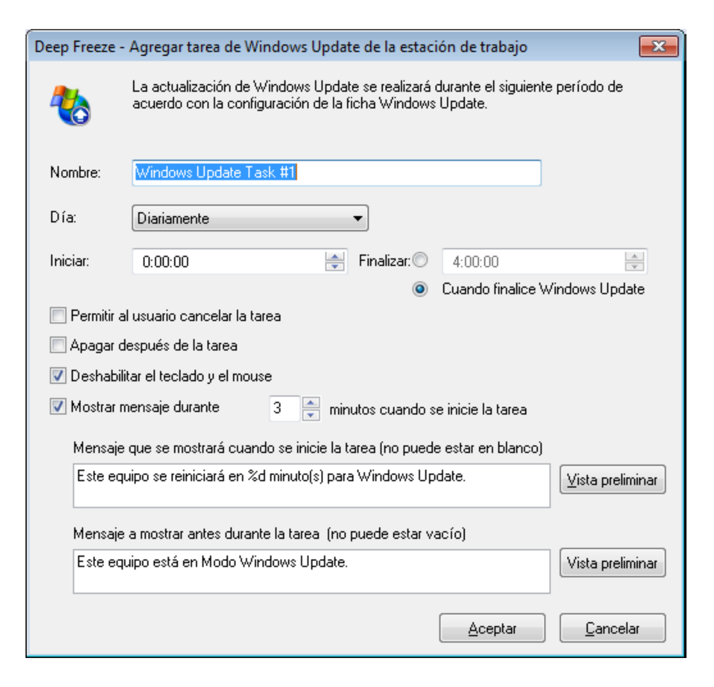
Las actualizaciones de Windows también se pueden aplicar manualmente en la estación de trabajo seleccionando la estación de trabajo y mediante el comando *Ejecutar actualización de Windows* del menú contextual de la consola Deep Freeze. Para obtener más información, consulte ***Gestión de Deep Freeze con la consola***.





Siga los pasos descritos a continuación para programar una tarea de actualización de Windows:

1. Seleccione *Actualización de Windows* en la lista desplegable *Tipo de tarea* y haga clic en *Agregar*.
2. Se mostrarán las opciones siguientes:



- *Nombre*: especifique un nombre para la tarea.
- *Día*: seleccione un día o especifique si la tarea debe llevarse a cabo entre semana o los fines de semana.



- *Inicio*: seleccione la hora de inicio.
- *Fin*: seleccione la hora de finalización. El intervalo mínimo es de 15 minutos. También puede seleccionar *Cuando finalice la actualización de Windows*. Si la tarea de actualización de Windows no se ha completado en un plazo de 6 horas, Deep Freeze finalizará la tarea.
- *Permitir al usuario cancelar la tarea*: seleccione esta casilla de verificación para permitir al usuario cancelar la tarea antes de que se inicie.
- *Apagar después de la tarea*: seleccione esta casilla de verificación para apagar el equipo después de la tarea.
- *Deshabilitar teclado y ratón*: seleccione esta casilla de verificación para deshabilitar el teclado y el ratón durante la tarea.
- *Mostrar mensaje*: seleccione esta casilla de verificación para mostrar un mensaje en el equipo *Antes* y *Durante* la tarea. Especifique un intervalo de tiempo en minutos e introduzca el mensaje que desea que se muestre antes de que se inicie la tarea.

3. Haga clic en Aceptar. Se mostrará la *Ficha Actualización de Windows* para que pueda configurar ajustes adicionales, si procede.



El campo *Mostrar este mensaje antes de la tarea* muestra el mensaje *Este equipo se reiniciará en %d para una tarea de actualización de Windows*. Es posible editar este mensaje. Agregue la palabra *minutos* en el mensaje después de *%d* para incluirla como parte del mensaje.



Cuando programe una tarea de actualización de Windows, seleccione la opción *Cuando finalice la actualización de Windows* o asegúrese de dejar un margen de tiempo suficiente para que se lleven a cabo todas las actividades de actualización necesarias. Consulte los boletines de seguridad de Microsoft en el sitio web Technet (http://technet.microsoft.com/es-es/security) para obtener información detallada sobre el margen de tiempo necesario para las actualizaciones críticas y de seguridad publicadas.



Si no utiliza WSUS, el proceso de actualización de Windows de Deep Freeze solo aplicará actualizaciones críticas y de seguridad que no requieran la intervención del usuario. Si utiliza WSUS, se aplicarán todas las actualizaciones aprobadas.

Para aplicar otras actualizaciones disponibles, también puede visitar el sitio web Catálogo de Microsoft Update (http://catalog.update.microsoft.com/v7/site/Install.aspx) para obtener descargas que podrá aplicar posteriormente con una tarea de estación de trabajo de archivo por lotes. Las tareas de archivo por lotes también permiten aplicar otras actualizaciones de software de terceros.



La configuración especificada en la ficha Actualización de Windows de Deep Freeze anula la configuración de actualización de Windows en la estación de trabajo.

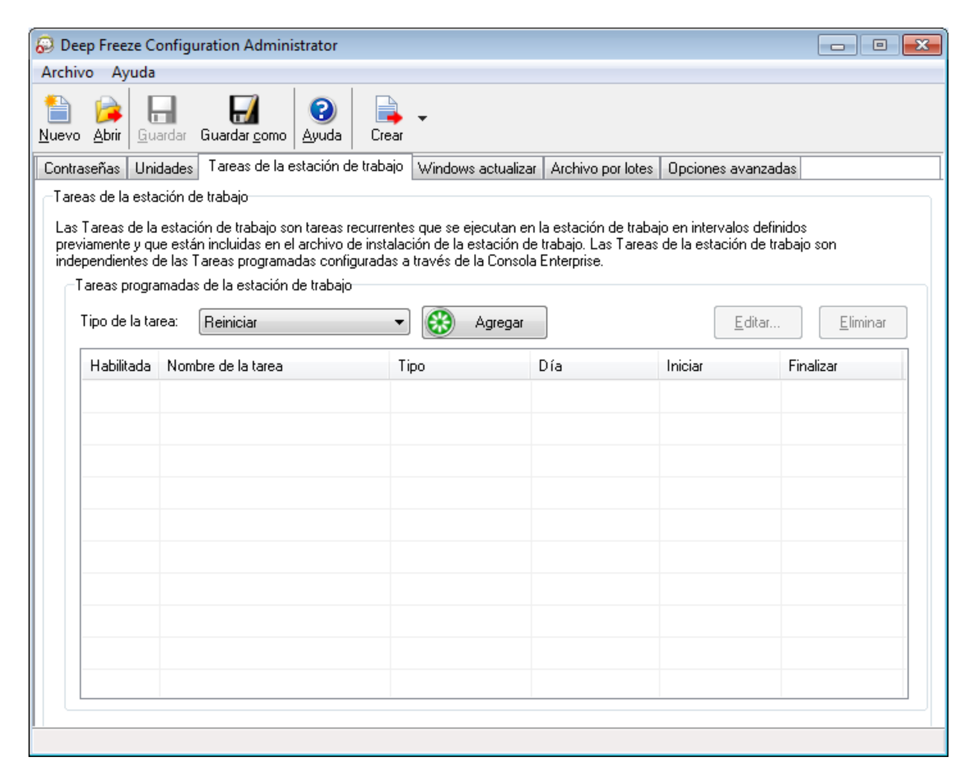


Ejemplo:

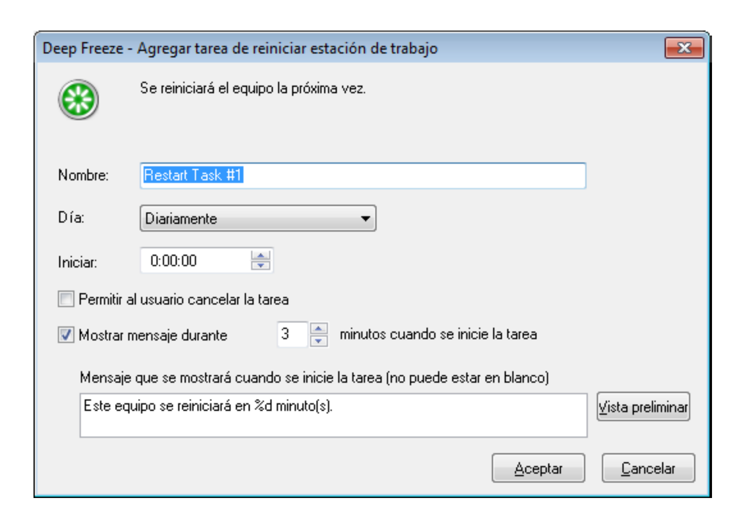
En la pantalla que se muestra arriba, se ha creado una tarea de actualización de Windows que se iniciará en el equipo todos los días a las 12:00 a.m. y finalizará cuando termine la *actualización de Windows*. Se ha configurado la tarea para que se muestre un mensaje al usuario antes de que se inicie la actualización de Windows. Se deshabilitarán el teclado y el ratón.

Reiniciar

Siga los pasos descritos a continuación para programar una tarea de reinicio:



1. Seleccione *Reiniciar* en la lista desplegable *Tipo de tarea* y haga clic en *Agregar*.
2. Se mostrarán las opciones siguientes:





- *Nombre*: especifique un nombre para la tarea.
- *Día*: seleccione un día o especifique si la tarea debe llevarse a cabo entre semana o los fines de semana.
- *Inicio*: seleccione la hora de inicio.
- *Permitir al usuario cancelar la tarea*: seleccione esta casilla de verificación para permitir al usuario cancelar la tarea antes de que se inicie.
- *Mostrar mensaje*: seleccione esta casilla de verificación para mostrar un mensaje en el equipo antes de que se inicie la tarea. Especifique un intervalo de tiempo en minutos e introduzca el mensaje que desea que se muestre antes de que se inicie la tarea.

3. Haga clic en Aceptar.



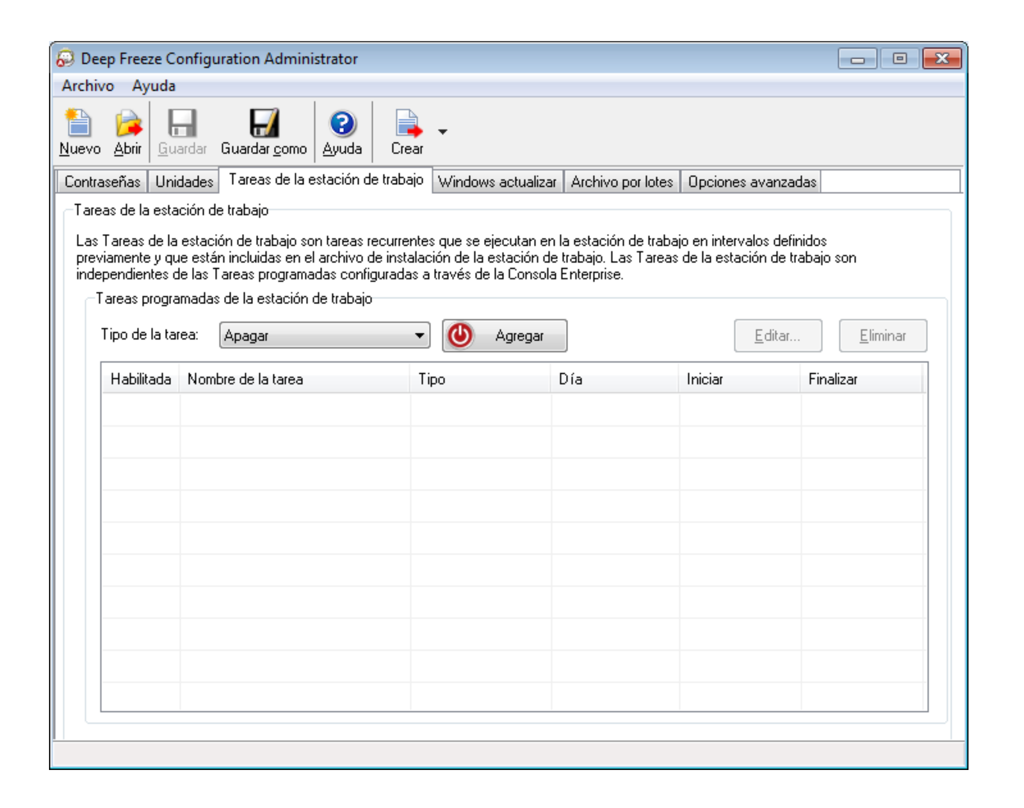
El campo *Mostrar este mensaje antes de la tarea* muestra el mensaje *Este equipo se reiniciará en %d*. Es posible editar este mensaje. Agregue la palabra *minutos* en el mensaje después de *%d* para incluirla como parte del mensaje.

Ejemplo:

En la pantalla que se muestra arriba, se ha creado una tarea de estación de trabajo para reiniciar el equipo diariamente a las 12:00 a.m. Se ha configurado la tarea para que se muestre un mensaje al usuario 1 minuto antes del reinicio.

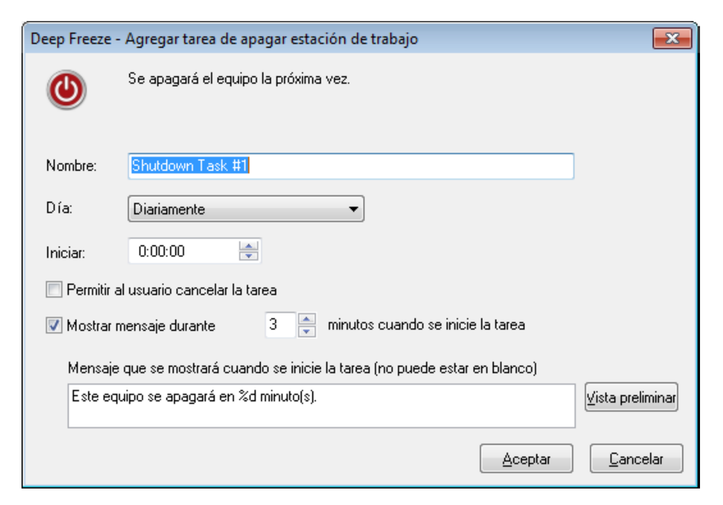
Apagar

Siga los pasos descritos a continuación para programar una tarea de apagado:





1. Seleccione *Apagar* en la lista desplegable *Tipo de tarea* y haga clic en *Agregar*.
2. Se mostrarán las opciones siguientes:



- *Nombre*: especifique un nombre para la tarea.
- *Día*: seleccione un día o especifique si la tarea debe llevarse a cabo entre semana o los fines de semana.
- *Inicio*: seleccione la *Hora de inicio*.
- *Permitir al usuario cancelar la tarea*: seleccione esta casilla de verificación para permitir al usuario cancelar la tarea antes de que se inicie.
- *Mostrar mensaje*: seleccione esta casilla de verificación para mostrar un mensaje en el equipo antes de que se inicie la tarea. Especifique un intervalo de tiempo en minutos e introduzca el mensaje que desea que se muestre antes de que se inicie la tarea.

3. Haga clic en Aceptar.



El campo *Mostrar este mensaje antes de la tarea* muestra el mensaje *Este equipo se apagará en %d*. Es posible editar este mensaje. Agregue la palabra *minutos* en el mensaje después de *%d* para incluirla como parte del mensaje.

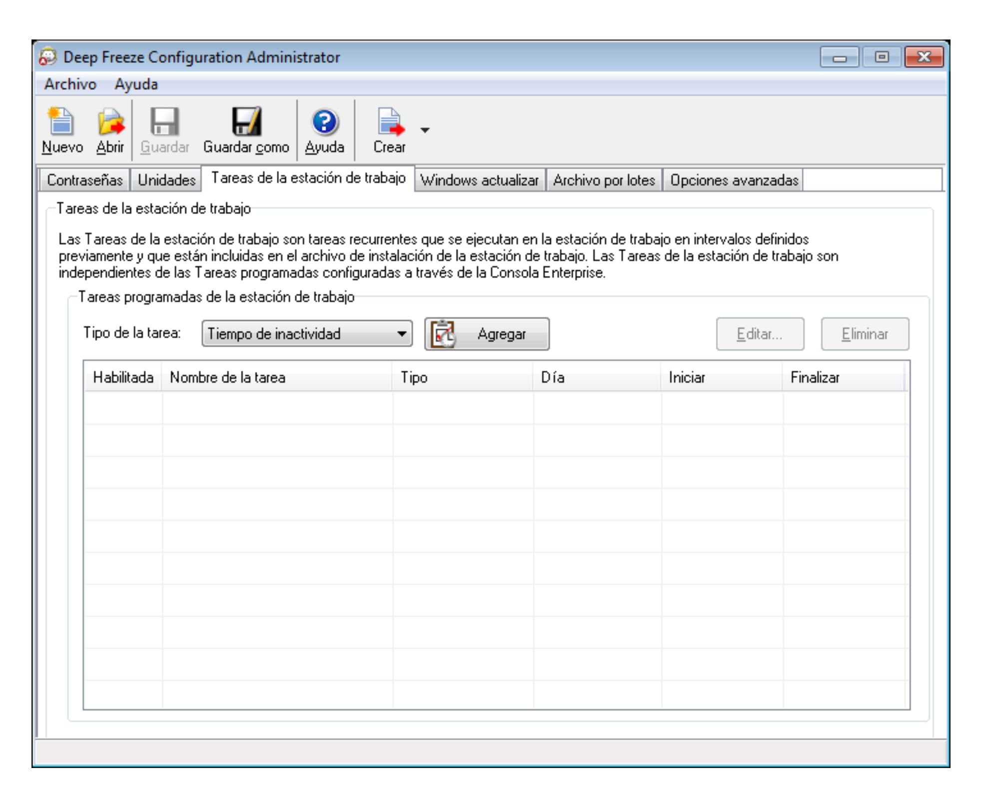
Ejemplo:

En la pantalla que se muestra arriba, se ha creado una tarea de apagado para reiniciar el equipo diariamente a las 12:00 a.m. Se ha configurado la tarea para que se muestre un mensaje al usuario 1 minuto antes del apagado.

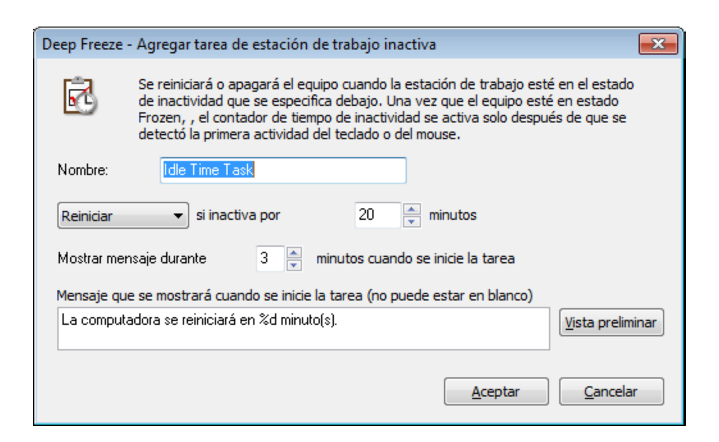
Tiempo de inactividad

Siga los pasos descritos a continuación para programar una tarea de tiempo de inactividad:





1. Seleccione *Tiempo de inactividad* en la lista desplegable *Tipo de tarea* y haga clic en *Agregar*.
2. Se mostrarán las opciones siguientes:



- *Nombre*: especifique un nombre para la tarea.
- *Reiniciar* o *Apagar*: seleccione *Reiniciar* o *Apagar* y especifique el tiempo de inactividad en minutos que debe transcurrir para que se lleve a cabo la tarea.
- *Mostrar mensaje*: active esta casilla de verificación para mostrar un mensaje. Especifique un intervalo de tiempo en minutos e introduzca un mensaje.



Una vez se haya iniciado el equipo, el contador de tiempo de inactividad se activará cuando se detecte actividad del teclado o del ratón. Durante una sesión de escritorio remoto, se utilizará el tiempo de inactividad del equipo de control para activar la tarea.



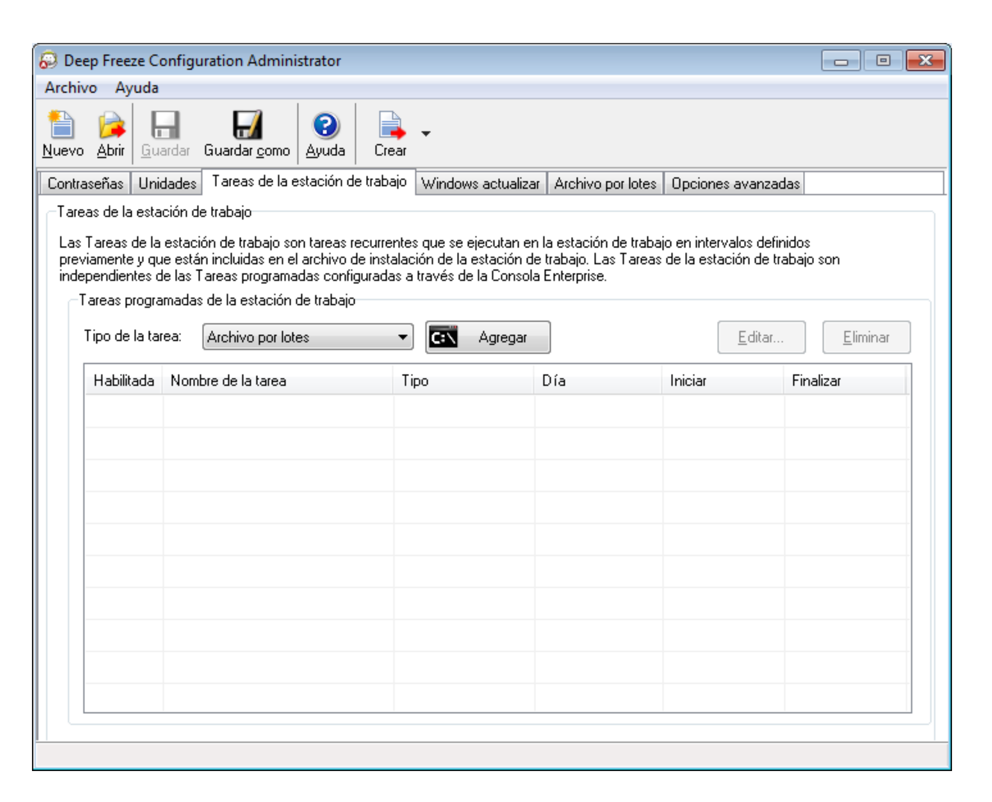
3. Haga clic en Aceptar.

Ejemplo:

En la pantalla que se muestra arriba, se ha configurado la tarea de tiempo de inactividad para *reiniciar* el equipo cuando esté inactivo durante 1 minuto. Se mostrará un mensaje al usuario durante 1 minuto después de que transcurra el tiempo de inactividad. El equipo se reiniciará a menos que el usuario cancele la tarea en el cuadro de diálogo mostrado.

Archivo por lotes

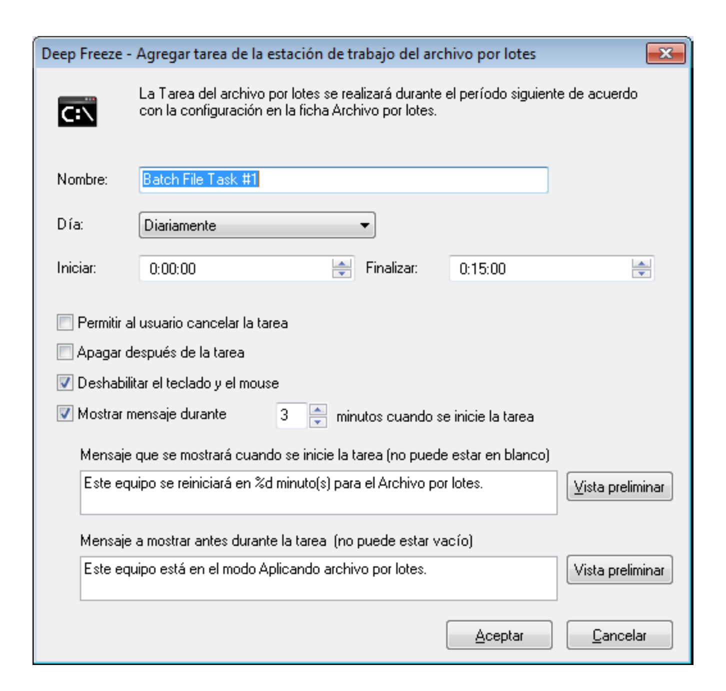
Las tareas de archivo por lotes permiten ejecutar archivos por lotes en la estación de trabajo. Una tarea de archivo por lotes tiene una hora de inicio y una hora de finalización. Durante este periodo, el archivo por lotes se ejecutará en la estación de trabajo. Es preciso configurar ajustes adicionales en la ficha Archivo por lotes para que se lleve a cabo la tarea de archivo por lotes. Puede configurar el equipo para que la estación de trabajo se apague cuando finalice la tarea de archivo por lotes. La estación de trabajo se reiniciará como *congelada* tras la ejecución del archivo por lotes.



Siga los pasos descritos a continuación para programar una tarea de archivo por lotes:

1. Seleccione *Archivo por lotes* en la lista desplegable *Tipo de tarea* y haga clic en *Agregar*.
2. Se mostrarán las opciones siguientes:





- *Nombre*: especifique un nombre para la tarea.
- *Día*: seleccione un día o especifique si la tarea debe llevarse a cabo entre semana o los fines de semana.
- *Inicio*: seleccione la hora de inicio.
- *Fin*: seleccione la hora de finalización. El intervalo mínimo es de 15 minutos.
- *Permitir al usuario cancelar la tarea*: seleccione esta casilla de verificación para permitir al usuario cancelar la tarea antes de que se inicie.
- *Apagar después de la tarea*: seleccione esta casilla de verificación para apagar el equipo después de la tarea.
- *Deshabilitar teclado y ratón*: seleccione esta casilla de verificación para deshabilitar el teclado y el ratón durante la tarea.
- *Mostrar mensaje*: seleccione esta casilla de verificación para mostrar un mensaje en el equipo *Antes* y *Durante* la tarea. Especifique un intervalo de tiempo en minutos e introduzca el mensaje que desea que se muestre antes de que se inicie la tarea.

3. Haga clic en Aceptar.
4. Vaya a la *Ficha Archivo por lotes* para configurar ajustes adicionales, si procede.



El campo *Mostrar este mensaje antes de la tarea* muestra el mensaje *Este equipo se reiniciará en %d para una tarea de archivo por lotes*. Es posible editar este mensaje. Agregue la palabra *minutos* en el mensaje después de *%d* para incluirla como parte del mensaje.

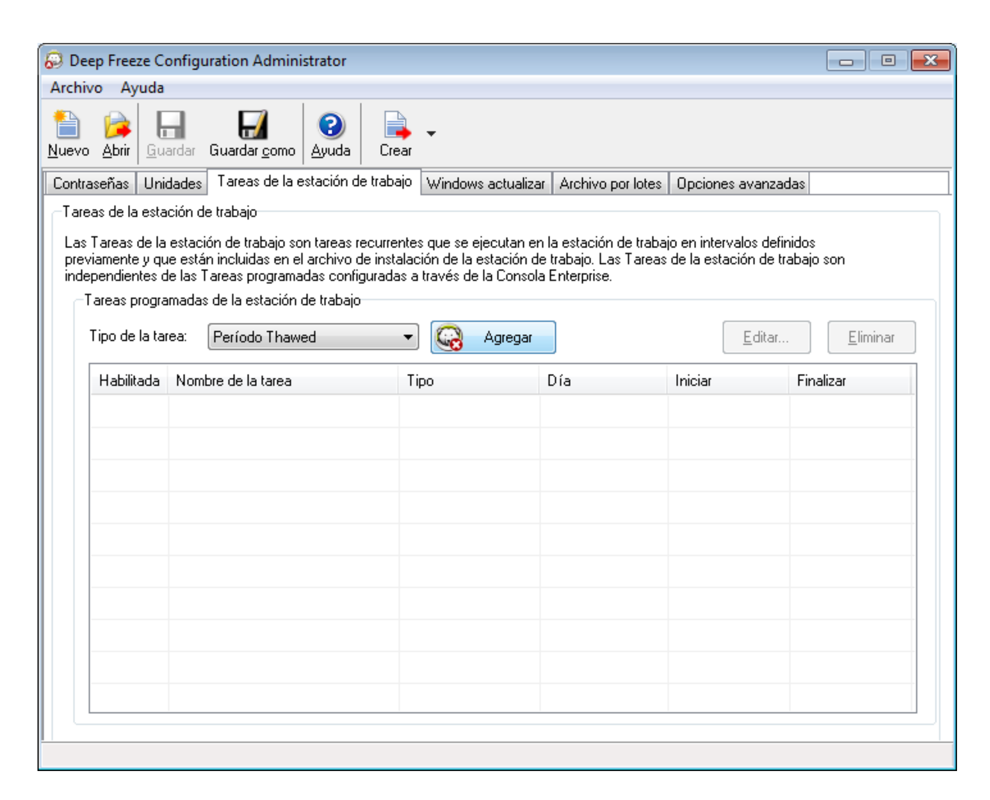


Ejemplo:

En la pantalla que se muestra arriba, se ha creado una tarea de archivo por lotes que ejecutará un archivo por lotes en el equipo diariamente a las 12:00 a.m y finalizará a las 12.15 a.m. Se ha configurado la tarea para que se muestre un mensaje al usuario antes de que se ejecute el archivo por lotes. Se deshabilitarán el teclado y el ratón.

Periodo de descongelación

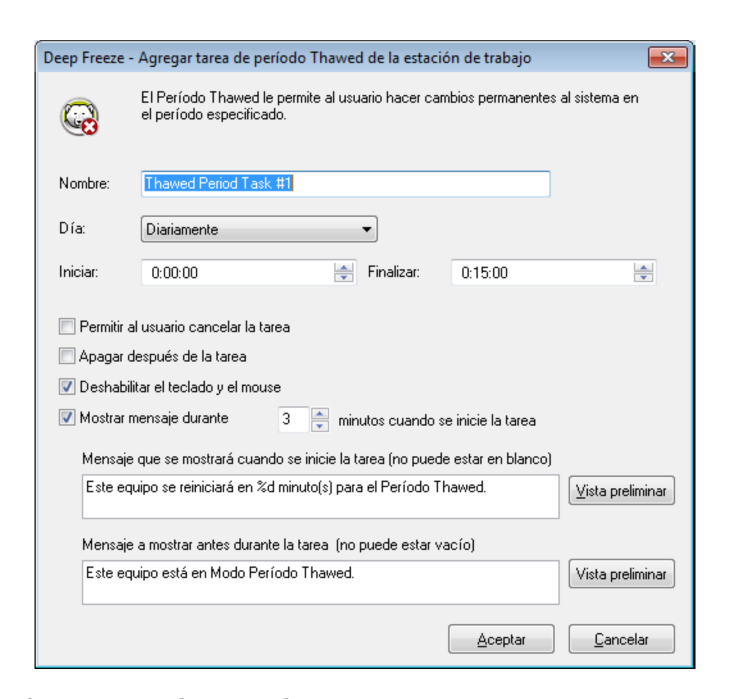
Las tareas de periodo de descongelación permiten reiniciar la estación de trabajo en modo Descongelado. Los periodos de descongelación son prácticos para aplicaciones que se actualizan automáticamente a intervalos regulares. También permiten a los administradores programar tareas de mantenimiento y realizar cambios permanentes en los equipos (p.ej., instalar nuevo software, actualizar software existente, configurar cambios y otras funciones de mantenimiento). Los periodos de descongelación tienen una hora de inicio y una hora de finalización.



Siga los pasos descritos a continuación para programar una tarea de periodo de descongelación:

1. Seleccione *Periodo de descongelación* en la lista desplegable *Tipo de tarea* y haga clic en *Agregar*.
2. Se mostrarán las opciones siguientes:





- *Nombre*: especifique un nombre para la tarea.
- *Día*: seleccione un día o especifique si la tarea debe llevarse a cabo entre semana o los fines de semana.
- *Inicio*: seleccione la hora de inicio.
- *Fin*: seleccione la hora de finalización. El intervalo mínimo es de 15 minutos.
- *Permitir al usuario cancelar la tarea*: seleccione esta casilla de verificación para permitir al usuario cancelar la tarea antes de que se inicie.
- *Apagar después de la tarea*: seleccione esta casilla de verificación para apagar el equipo después de la tarea.
- *Deshabilitar teclado y ratón*: seleccione esta casilla de verificación para deshabilitar el teclado y el ratón durante la tarea.
- *Mostrar mensaje*: seleccione esta casilla de verificación para mostrar un mensaje en el equipo *Antes* y *Durante* la tarea. Especifique un intervalo de tiempo en minutos e introduzca el mensaje que desea que se muestre antes de que se inicie la tarea.

3. Haga clic en Aceptar.



El campo *Mostrar este mensaje antes de la tarea* muestra el mensaje *Este equipo se reiniciará en %d para una tarea de mantenimiento*. Es posible editar este mensaje. Agregue la palabra *minutos* en el mensaje después de *%d* para incluirla como parte del mensaje.

Ejemplo:

Los programas antivirus necesitan actualizaciones regulares de las definiciones para proteger el sistema. Las definiciones de virus se pueden actualizar durante un período de descongelación.



En la pantalla que se muestra arriba, se ha creado una tarea del periodo de descongelación todos los días entre 12:00 a.m. y 12:15 a.m. El usuario no está autorizado a cancelar la tarea antes de que comience. El equipo se apagará después del periodo de mantenimiento. El teclado y ratón se deshabilitarán durante el periodo de mantenimiento. Se ha configurado la tarea para que se muestre un mensaje al usuario 5 minutos antes de que se inicie la tarea. Se mostrará el siguiente mensaje en el equipo a las 11:55 a.m. *El equipo se reiniciará en 5 minutos para entrar en modo de descongelación.*

Para asegurarse de que las definiciones de virus se apliquen de forma permanente, programe la actualización de las definiciones de virus de su programa antivirus de manera que se *inicie* después de que Deep Freeze inicie la tarea de periodo de descongelación y *finalice* antes de que Deep Freeze finalice la tarea de periodo de descongelación. Esto garantizará que las definiciones descargadas y actualizadas por el programa Anti-Virus se conserven permanentemente en el sistema. De este modo, el sistema estará completamente protegido por Anti-Virus y Deep Freeze.



Faronics Anti-Virus: Faronics Anti-Virus trabaja con Deep Freeze y no requiere una tarea de periodo de descongelación para actualizar las definiciones de virus. Faronics Anti-Virus puede actualizar las definiciones de virus aunque los equipos gestionados con Deep Freeze estén en modo *Congelado*.

Otros programas antivirus: para poder actualizar las definiciones de virus de otros programas antivirus, deberá programar una tarea de periodo de descongelación. Consulte el manual del usuario de su programa antivirus para obtener información sobre la descarga de definiciones de virus. Otra alternativa es aplicar las definiciones de virus de forma manual cuando los equipos gestionados con Deep Freeze estén en modo *Descongelado*. También puede programar la instalación de definiciones de virus *sin intervención del usuario* mediante una tarea de archivo por lotes.

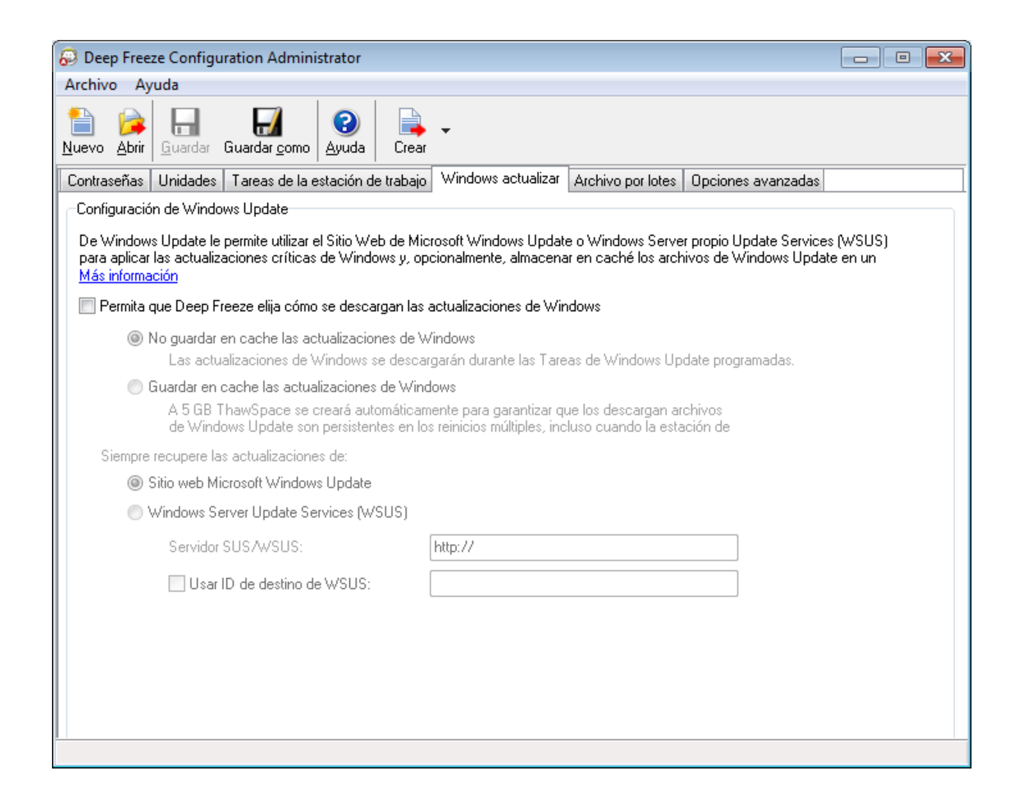


Ficha Actualización de Windows

Esta ficha permite personalizar la configuración de las actualizaciones de Windows. La primera vez que cree una tarea de actualización de Windows, podrá modificar la configuración predeterminada de la ficha Actualización de Windows. No es obligatorio modificar la configuración predeterminada. La actualización de Windows se llevará a cabo aunque no se modifique la configuración predeterminada. La configuración especificada en la ficha Actualización de Windows se aplicará a todas las tareas de actualización de Windows.



La configuración especificada en la ficha Actualización de Windows de Deep Freeze anula la configuración de actualización de Windows en la estación de trabajo.



Es posible personalizar los siguientes ajustes de la ficha Actualización de Windows:

Permitir a Deep Freeze elegir cómo se descargarán las actualizaciones de Windows: : seleccione esta casilla de verificación para permitir a Deep Freeze elegir la forma en la que se deben descargar las actualizaciones de Windows. Estas son las opciones disponibles:



- Seleccione las opciones de descarga de las actualizaciones de Windows:
  - *No almacenar en caché actualizaciones de Windows*: seleccione esta opción para descargar las actualizaciones de Windows solo durante una tarea de actualización de Windows.
  - *Almacenar en caché actualizaciones de Windows*: seleccione esta opción para descargar las actualizaciones de Windows cuando la estación de trabajo esté en modo Congelado o Descongelado e instalarlas durante una tarea de actualización de Windows. Esta opción crea un ThawSpace de 4 GB donde se almacenarán las actualizaciones de Windows para garantizar que los archivos de actualización de Windows se mantengan tras varios reinicios.
- Recuperar siempre actualizaciones de:
  - *Sitio web de Microsoft Windows Update*: seleccione esta opción para descargar las actualizaciones directamente del sitio web de Microsoft Windows Update.
  - *Windows Server Update Services (WSUS)* : seleccione esta opción para descargar las actualizaciones del servidor WSUS. Especifique el *Servidor SUS/WSUS*. También puede seleccionar *Usar destino WSUS* y especificar un destino. Puede descargar el cliente Microsoft SUS y el servidor SUS/WSUS en: http://www.microsoft.com/wsus.



Se creará un archivo de registro para cada una de las estaciones de trabajo y se almacenará localmente en la estación de trabajo.

El nombre predeterminado para el archivo de registro de actualizaciones de Windows de Deep Freeze es *DFWuLogfile.log*, y puede encontrarse en la ubicación siguiente:

C:\Archivos de programa\Faronics\Deep Freeze\Install C-[X]\DFWuLogfile.log (sistema de 32 bits) y C:\Program Files (x86)\Faronics\Deep Freeze\Install C-[X]\DFWuLogfile.log (sistemas de 64 bits).

- No es posible cambiar el nombre ni la ubicación del archivo de registro.
- El archivo de registro de Deep Freeze y el archivo de registro de actualizaciones de Windows (en c:\windows\windowsupdate.log) permiten solucionar problemas relacionados con las actualizaciones de Windows.
- X es un valor incremental, que variará en función de las veces que haya instalado Deep Freeze en la estación de trabajo.

Póngase en contacto con el servicio de soporte de Faronics en http://support.faronics.com para obtener información detallada sobre cómo solucionar problemas con el registro DFWuLogfile.log.

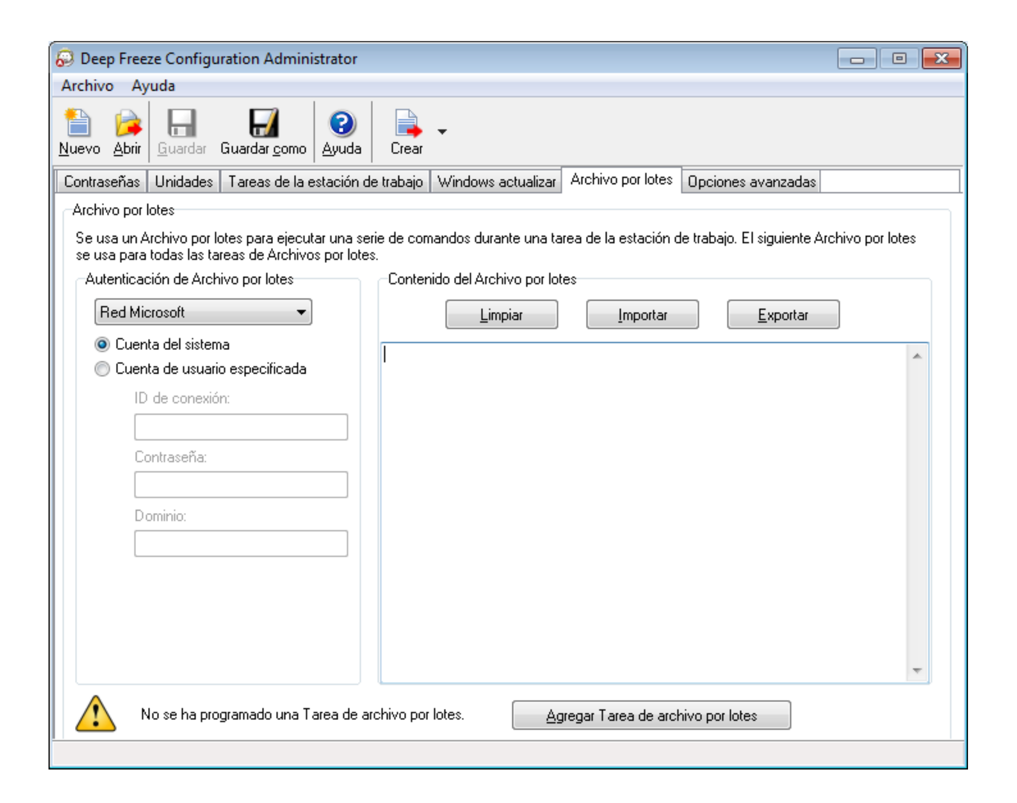
Póngase en contacto con el servicio de soporte de Microsoft para obtener información sobre como solucionar problemas de actualización de Windows. (Visite http://support.microsoft.com/kb/906602)

Lea también el artículo 902093 *Cómo leer el archivo Windowsupdate.log* en: http://support.microsoft.com/kb/902093/ o visite http://support.microsoft.com/?ln=es-es.



Ficha Archivo por lotes

La ficha Archivo por lotes permite personalizar la configuración de las tareas de archivo por lotes. Cuando programe una tarea de archivo por lotes en la ficha Tareas de estación de trabajo, deberá configurar los ajustes en la ficha Tarea por lotes.



Configure las opciones siguientes:

- Autenticación de archivo por lotes

  Seleccione Microsoft Network y especifique si la cuenta que se va a utilizar es una cuenta del sistema o una cuenta especificada por el usuario. Si selecciona una cuenta especificada por el usuario, introduzca el Id. de inicio de sesión, la contraseña y el dominio. Para una red Novell, seleccione Novell, especifique el Id. de inicio de sesión, la contraseña, el árbol, el contexto y el servidor.



Es preciso probar la configuración predeterminada con la autenticación de cuenta del sistema/Microsoft Network antes de usar credenciales alternativas. El uso de esta cuenta de nivel del sistema suele ser suficiente para completar la tarea. Es posible que se deba utilizar una cuenta de usuario específica si el archivo por lotes requiere acceso de red a recursos protegidos.

- Contenido de archivo por lotes



Introduzca el archivo por lotes personalizado que se vaya a ejecutar durante la tarea de archivo por lotes. El archivo por lotes especificado se aplicará a todas las tareas de archivo por lotes. Están disponibles las opciones siguientes:

— Para borrar el archivo por lotes actual, haga clic en *Borrar*.

— Para cargar un archivo por lotes, haga clic en *Importar* y especifique la ubicación del archivo.

— Para guardar el contenido del archivo, haga clic en *Exportar* y seleccione la ubicación donde desee guardar el archivo.

El archivo por lotes puede contener cualquier comando o serie de comandos que pueda ejecutar el procesador de comandos. Puede ejecutar secuencias de comandos personalizadas que requieran el uso de motores de secuencias de comandos de terceros llamando la secuencia de comandos desde el archivo por lotes como si se estuviera ejecutando desde la línea de comandos.

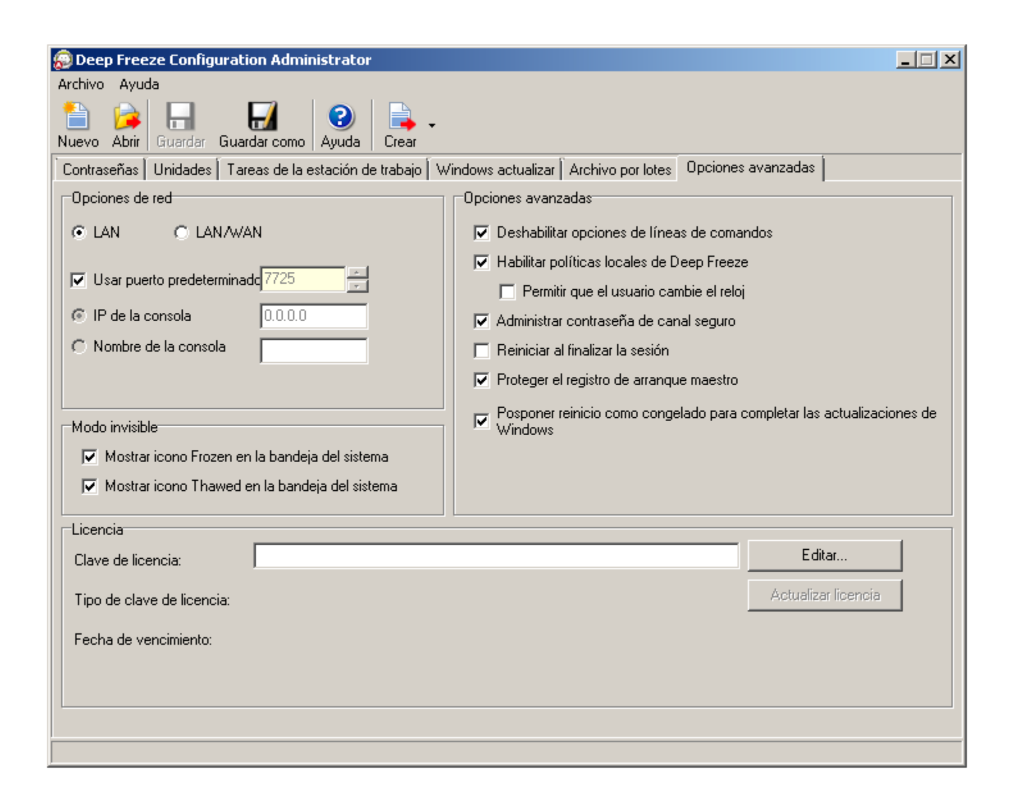


Los archivos por lotes permiten utilizar secuencias de comandos de Visual Basic, PowerShell, Niite y otras soluciones de terceros. Póngase en contacto con su proveedor de software o consulte la documentación de su solución para obtener más información acerca de las soluciones de secuencias de comandos que incluyen opciones que *no requieren la intervención del usuario*.



Ficha Opciones avanzadas

La ficha Opciones avanzadas permite configurar los ajustes de red usados por los equipos para comunicarse con la consola, configurar diferentes opciones de seguridad y administrar las claves de licencia.



Red

La consola Deep Freeze Enterprise puede comunicarse con los equipos que tienen Deep Freeze instalado mediante dos modos distintos: modo LAN o modo LAN/WAN.

- LAN: Seleccione LAN para que Deep Freeze se comunique dentro de una red de área local (LAN). El modo LAN es un modo de configuración automática que solamente requiere un número de puerto. El puerto predeterminado es el 7725. El número de puerto puede cambiarse si entra en conflicto con otros programas en la red de área local. En el modo LAN, los equipos de destino con Deep Freeze y la consola Enterprise se encuentran entre sí mediante transmisiones UDP. Estas transmisiones solamente ocurren al iniciar el equipo o la consola Enterprise con el fin de minimizar el tráfico de red asociado con la comunicación entre el equipo de destino y la consola.
- LAN/WAN: seleccione LAN/WAN para que Deep Freeze se comunique tanto en una LAN como en una WAN (red de área amplia). Se puede utilizar LAN/WAN en un entorno LAN o WAN, y en Internet. Este modo utiliza una dirección IP o el nombre del equipo, junto con un número de puerto, para permitir la comunicación entre la consola Enterprise y los equipos gestionados.

Los dos métodos siguientes permiten la identificación de la consola:



- Especificar la IP de la consola (debe ser estática)
- Especificar el nombre de la consola (en ese caso, la IP puede ser dinámica si la resolución de nombres DNS está disponible como parte de la infraestructura del dominio).

Si la consola Enterprise está protegida por un firewall o un enrutador NAT (Network Address Translation o traducción de direcciones de red), es preciso configurar el firewall o enrutador para que permitan el paso del tráfico a través de la consola Enterprise. En función del firewall o enrutador, es posible que los equipos deban configurarse con la dirección IP del firewall para que pueda reenviarse el tráfico.



Deep Freeze configura automáticamente las excepciones necesarias en el firewall de Windows. No es preciso configurar el firewall de Windows manualmente.

Para obtener más información acerca de la configuración y el uso de Deep Freeze en un entorno de red específico, consulte el *Apéndice B* o póngase en contacto con el equipo de soporte técnico.

Si se utiliza un número de puerto distinto del 7725 predeterminado (registrado para Deep Freeze), hay que tener cuidado de que no se produzcan conflictos con las aplicaciones que ya se están ejecutando en la red. Se deben evitar los puertos conocidos (0–1023) y se debe comprobar que no haya conflictos en los puertos registrados (1024–49151) antes de la implementación.



Se recomienda utilizar puertos en el rango no asignado superior a 49152. La segmentación de puertos permite aislar una sala o edificio por número de puerto al configurar el número de puerto en las estaciones de trabajo y en la consola Deep Freeze Enterprise. Con este método, puede proporcionar funciones de gestión para un conjunto específico de estaciones de trabajo (no para toda la organización). Se requieren excepciones de puerto UDP y TCP para estos puertos. Para obtener más información, consulte *Ejemplo 3: varios puertos, acceso remoto a consola*.

Encontrará un listado completo de los puertos asignados a distintas aplicaciones en el sitio web de la Internet Assigned Numbers Authority en *http://www.iana.org/assignments/port-numbers*.

Opciones avanzadas

- *Deshabilitar opciones de línea de comandos*: esta opción está activada de forma predeterminada. La desactivación de esta casilla de verificación permite una mayor personalización del programa de instalación de Deep Freeze cuando se utiliza el sistema de instalación silenciosa. Si se selecciona esta opción, no se podrán cambiar las opciones de configuración preexistentes durante la instalación.
- *Habilitar directivas locales de Deep Freeze*: para mayor seguridad, Deep Freeze eliminará los siguientes privilegios locales: depuración de programas, modificación de firmware y cambio de la hora del sistema; desactive esta opción para utilizar los privilegios existentes.
- *Permitir al usuario cambiar el reloj*: seleccione esta opción para permitir a los usuarios congelados ajustar el reloj del sistema. Habilite esta opción durante el horario de verano para que Windows actualice la hora automáticamente cada estación.
- *Gestionar contraseña de canal seguro*: la contraseña de canal seguro es una característica de todos los sistemas operativos Windows y solo se aplica si el sistema se está ejecutando en un entorno de dominio de Windows Server. La contraseña de canal seguro permite proteger las comunicaciones entre el servidor y las estaciones de trabajo, y se cambia automáticamente de acuerdo con la configuración del sistema operativo. Mientras se utiliza Deep Freeze, la contraseña de canal seguro modificada se pierde al reinicio. La opción *Gestionar contraseña de canal seguro* evita esta situación. Esta función de Deep Freeze cambia el valor de la



directiva de grupo *Duración máxima de contraseña de cuenta de equipo* en función de si Deep Freeze está en modo *Congelado* o *Descongelado*.

— Seleccione la opción *Gestionar contraseña de canal seguro* si desea que Deep Freeze gestione la contraseña de canal seguro.

Si la estación de trabajo está en modo Congelado: la estación de trabajo no cambiará la contraseña de canal seguro. Esto garantiza que siempre se establezca una comunicación segura entre el servidor y la estación de trabajo.

Si la estación de trabajo está en modo Descongelado: la estación de trabajo cambiará la contraseña de canal seguro y la sincronizará con el servidor.

— No seleccione la opción *Gestionar contraseña de canal seguro* si no desea que Deep Freeze gestione la contraseña de canal seguro.

Si la estación de trabajo está en modo Congelado: una vez se haya cambiado la contraseña de canal seguro y se haya sincronizado con el servidor, se restablecerá la antigua contraseña al reiniciar.

Si la estación de trabajo está en modo Descongelado: si la estación de trabajo está en modo *Descongelado* el día que cambie la contraseña de canal seguro, se aplicará la nueva contraseña y la estación de trabajo se sincronizará con el servidor.



La función Gestionar contraseña de canal seguro de Deep Freeze anula la directiva de grupo *Duración máxima de contraseña de cuenta de equipo*.

Establezca lo siguiente en la directiva de grupo para garantizar el funcionamiento de Gestionar contraseña de canal seguro:

Controlador de dominio: no permitir los cambios de contraseña de cuenta de equipo (*No definido*)

- *Reiniciar al cerrar sesión*: seleccione esta casilla de verificación para *Reiniciar* el equipo automáticamente cuando se cierre la sesión. Si se selecciona esta opción, el equipo se reiniciará cuando el usuario cierre la sesión en modo Congelado.
- *Proteger registro de arranque principal*: active esta casilla de verificación si desea que Deep Freeze proteja el registro de arranque principal (Master Boot Record, MBR). Si se activa está opción, los cambios en el registro de arranque principal se revertirán al inicio cuando el equipo esté en modo *Congelado*.
- *Posponer reinicio como congelado para completar las actualizaciones de Windows*: seleccione esta opción para posponer el reinicio en modo Congelado si la configuración o instalación de las actualizaciones de Windows están pendientes durante una tarea de actualización de Windows. Si se selecciona esta opción y se realizan las actualizaciones de Windows (a través de medios distintos de Deep Freeze), el reinicio en modo Congelado garantiza que se complete la configuración e instalación de todas las actualizaciones de Windows antes de reiniciar en modo Congelado.





Si selecciona *Posponer reinicio como congelado para completar las actualizaciones de Windows* e instala Deep Freeze, el instalador comprobará si se han completado todas las actualizaciones de Windows. Si no se han completado, no se llevará a cabo la instalación de Deep Freeze. Complete las actualizaciones de Windows y pruebe a instalar Deep Freeze de nuevo.

Si desactiva *Posponer reinicio como congelado para completar las actualizaciones de Windows* e instala Deep Freeze, asegúrese de que todas las actualizaciones de Windows se han completado manualmente. Si desactiva esta opción, el equipo puede quedar atrapado en un ciclo de reinicios debido a las actualizaciones de Windows incompletas.

Ejemplo:

En un entorno de dominio de Windows con Windows Server 2008 R2 que administra varias estaciones de trabajo, la contraseña de canal seguro permite la comunicación segura entre el servidor y las estaciones de trabajo.

En el Administrador de configuración de Deep Freeze, vaya a la ficha *Opciones avanzadas* y seleccione *Gestionar contraseña de canal seguro*. Cree el archivo de instalación de estación de trabajo e impleméntelo en la estación de trabajo.

Establezca lo siguiente en la directiva de grupo para garantizar el funcionamiento de Gestionar contraseña de canal seguro:

Controlador de dominio: no permitir los cambios de contraseña de cuenta de equipo (*No definido*)

Miembro de dominio: deshabilitar los cambios de contraseña de cuenta de equipo (*Deshabilitar*)

Si la estación de trabajo está en modo Congelado, la contraseña de canal seguro no cambia. Si la estación de trabajo está en modo Descongelado, la contraseña de canal seguro cambia en la estación de trabajo y se sincroniza con el servidor.

Modo invisible

- *Mostrar icono Congelado en la bandeja del sistema*: seleccione esta opción para mostrar el icono que indica que Deep Freeze está instalado y que el equipo está en modo Congelado.
- *Mostrar icono Descongelado en la bandeja del sistema*: seleccione esta opción para mostrar el icono que indica que Deep Freeze está instalado y que el equipo está en modo Descongelado.

Si las opciones para mostrar el icono de Deep Freeze en la bandeja del sistema están desactivadas, se tendrá que utilizar el método abreviado CTRL+ALT+Mayús+F6 para acceder al cuadro de diálogo de inicio de sesión.

Licencia

- *Clave de licencia*: haga clic en *Editar* e introduzca la clave de licencia.
- *Tipo de clave de licencia*: muestra el tipo de clave de licencia. Este campo muestra si esta versión es una evaluación o una versión completa.
- *Fecha de caducidad*: muestra la *Fecha de caducidad* para Deep Freeze.



La clave de licencia se puede actualizar de las siguientes maneras:

— A través del archivo de instalación de estación de trabajo: la clave de licencia se actualizará en el Administrador de configuración y se creará el archivo de instalación de estación de trabajo. Ahora la clave de licencia es parte del archivo de instalación de estación de trabajo.

— A través de la consola Enterprise: la clave de licencia puede actualizarse directamente en la consola Enterprise. Si la clave de licencia se actualiza en la consola Enterprise, se actualizará automáticamente en todos los equipos conectados. Para obtener más información sobre cómo actualizar directamente a través de la consola Enterprise, consulte la sección *Licencia*.

— Manualmente en cada equipo: la clave de licencia puede actualizarse manualmente en cada equipo. Para obtener más información, consulte la sección *Ficha Estado*.



Al descargar las actualizaciones de la versión de Deep Freeze Enterprise en www.faronicslabs.com, recuerde que tendrá que copiar y pegar la clave de licencia más reciente de su cuenta para utilizarla en la instalación. Faronics actualiza la clave de licencia con cada revisión del software. Su cuenta de Faronics Labs se actualizará con la nueva clave de licencia en cada versión.



Creación de un programa de instalación de estación de trabajo y una semilla de estación de trabajo

Para crear archivos de programa de instalación de Deep Freeze personalizados con todas las opciones configuradas en las secciones anteriores, haga clic en el botón *Crear* en la barra de herramientas del Administrador de configuración y seleccione *Crear programa de instalación de estación de trabajo*.



El nombre de archivo predeterminado para este programa es DFWks.exe. Le recomendamos que mantenga el nombre predeterminado, pero es posible que en grandes implementaciones desee añadir como sufijo información relacionada con su configuración como, por ejemplo: *DFwks_10gbThawSpace.exe* o *DFWks_SinMantenimiento.exe* o *DFwks_Mie-5pmActualizaciones.exe* para ayudar en la organización y la identificación de las funciones del instalador. La misma recomendación se aplica para los archivos de *configuración de Deep Freeze* (.rdx).

Este archivo puede utilizarse posteriormente para instalar Deep Freeze en los equipos mediante:

- Instalación con supervisión (instalación basada en los datos provistos por el usuario)
- Sistema de instalación silenciosa (la instalación no informa al usuario del progreso ni le muestra mensajes durante la instalación). Para obtener más información acerca de los comandos de instalación silenciosa, consulte Instalación o desinstalación silenciosa, página 101.
- Instalación localizada: mediante la consola Deep Freeze Enterprise para estaciones de trabajo que ya contienen una semilla o una versión previa de Deep Freeze creada con el mismo código de personalización.

Para crear una semilla de estación de trabajo, haga clic en el botón *Crear*en la barra de herramientas del Administrador de configuración y seleccione *Crear semilla de estación de trabajo*. La semilla de estación de trabajo es un programa ligero que permite a los administradores instalar y controlar los equipos de forma remota desde la consola Enterprise. La semilla de estación de trabajo puede instalarse como parte de una imagen maestra y luego implementarse a través del software de imágenes de disco. Todos los equipos en la LAN con la semilla de estación de trabajo instalada se mostrarán en la consola Enterprise. El nombre predeterminado de este programa es *DFWksSeed.exe*.

Todos los archivos se guardan en la carpeta *Deep Freeze Enterprise*/*Install Programs* de forma predeterminada. Es posible elegir una ubicación diferente y cambiar el nombre de archivos, si es necesario. Se recomienda utilizar una convención para la nomenclatura si se tiene previsto crear varios archivos de instalación personalizados.





Los archivos *DFwks.exe*, *DFwksseed.exe,* y *depfrz.rdx* se pueden crear e implementar de manera intercambiable en cualquier equipo de Deep Freeze que utilice el mismo código de personalización. La semilla de Deep Freeze se puede utilizar como una plantilla o marcador de posición para garantizar la coherencia de los elementos básicos como contraseñas, configuración de red o tareas de estación de trabajo estandarizadas. La semilla no utilizará ninguno de los ajustes de configuración, sino que los mantendrá en el archivo. Para utilizar el archivo como una plantilla, simplemente abra el archivo *DFwksseed.exe* con el Administrador de configuración y realice los cambios pertinentes. A continuación, haga clic en *Crear*> *Crear archivo de instalación de estación de trabajo* para crear el archivo de instalación de estación de trabajo.





Se recomienda restringir el uso del Administrador de configuración en entornos más grandes por razones de seguridad. Puede hacerlo protegiendo con contraseña el Administrador de Deep Freeze o eliminando el archivo DFadmin.exe de la carpeta *c:\archivos de programa\faronics\Deep Freeze 7 Enterprise*. Este archivo puede moverse a la estación de trabajo del Administrador de dominios y eliminarse de la consola Deep Freeze Enterprise común. Para restaurarlo cópielo de otra instalación con la misma versión y proporcione autorización con la contraseña OTP o mediante la reinstalación o actualización de Deep Freeze Enterprise con el mismo código de personalización.



Uso de la consola Deep Freeze Enterprise

En este capítulo se describe cómo utilizar la consola Deep Freeze Enterprise.

Temas

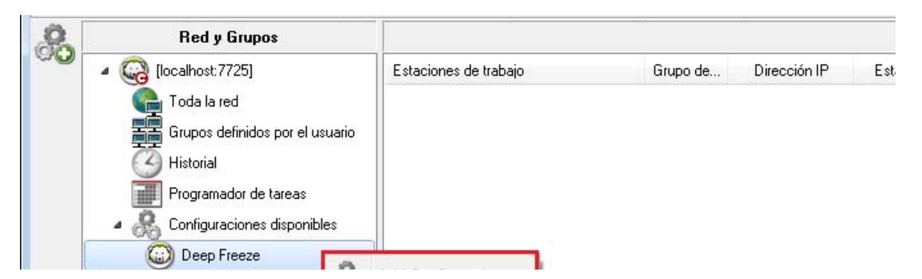


Configuración de Deep Freeze

La configuración de Deep Freeze es un grupo de ajustes que definen el comportamiento de Deep Freeze en la estación de trabajo. Las configuraciones de Deep Freeze se pueden crear y aplicar a través de la consola Deep Freeze.

Siga los pasos descritos a continuación para crear una configuración de Deep Freeze:

1. Inicie la consola Deep Freeze..
2. Vaya a *Red y grupos* > *Configuraciones disponibles* > *Deep Freeze*.
3. Haga clic con el botón secundario y seleccione *Crear nueva configuración*.



4. Seleccione o especifique los ajustes en cada ficha como se describe en *Utilización del Administrador de configuración de Deep Freeze*.
5. Haga clic en *Aceptar*.
6. Especifique el nombre de la configuración y haga clic en *Aceptar*.

Aplicar la configuración de Deep Freeze

Una vez creada la configuración, se puede aplicar a varias estaciones de trabajo.

Siga los pasos descritos a continuación para aplicar la configuración de Deep Freeze:

1. Vaya al panel *Estaciones de trabajo*.
2. Seleccione una o más estaciones de trabajo.
3. Haga clic con el botón secundario y seleccione *Actualizar configuración* > *Deep Freeze* > *[Nombre de la configuración]*.

La configuración se aplicará a las estaciones de trabajo seleccionadas.

Editar la configuración de Deep Freeze

Siga los pasos descritos a continuación para editar la configuración de Deep Freeze:

1. Vaya al panel Red y grupos en la consola Enterprise.
2. Seleccione *Configuraciones disponibles* > *Deep Freeze* > *[Nombre de la configuración]*.
3. Haga clic con el botón secundario en la configuración seleccionada y seleccione *Editar configuración seleccionada*.
4. Edite la configuración según sea necesario.
5. Haga clic en *Aceptar*.



Eliminar la configuración de Deep Freeze

Siga los pasos descritos a continuación para eliminar la configuración de Deep Freeze:

1. Vaya al panel Red y grupos en la consola Enterprise.
2. Seleccione *Configuraciones disponibles* > *Deep Freeze* > *[Nombre de la configuración].*
3. Haga clic con el botón secundario en la configuración seleccionada y seleccione *Eliminar configuración seleccionada*.
4. Haga clic en *Aceptar*.

Exportar la configuración de Deep Freeze

Siga los pasos descritos a continuación para exportar la configuración de Deep Freeze:

1. Vaya al panel Red y grupos en la consola Enterprise.
2. Seleccione *Configuraciones disponibles* > *Deep Freeze* > *[Nombre de la configuración].*
3. Haga clic con el botón secundario en la configuración seleccionada y seleccione *Exportar como*. Hay tres opciones disponibles:

- Seleccionar instalador de estación de trabajo. Especifique un nombre y haga clic en *Guardar*.
- Seleccionar semilla de estación de trabajo. Especifique un nombre y haga clic en *Guardar*.
- Seleccionar archivo de configuración. Especifique un nombre y haga clic en *Guardar*.



Consola Deep Freeze Enterprise

La consola Deep Freeze Enterprise muestra el estado de todos los equipos en modo Congelado, Descongelado y Destino de la red y permite al administrador ejecutar ciertas tareas en dichos equipos. La información de estado detallada se encuentra disponible mediante la generación de informes grupales o selectivos.

La consola Enterprise permite a los administradores realizar las siguientes tareas de forma remota:

- Realizar de inmediato la instalación localizada en equipos
- Poner en modo Congelado, Descongelado o Descongelado y bloqueado uno o más equipos de forma selectiva.
- Bloquear o desbloquear los equipos seleccionados
- Reiniciar o apagar los equipos
- Detener el mantenimiento programado
- Encender los equipos con una tarjeta de red Wake-on-LAN
- Actualizar el software Deep Freeze
- Programar tareas directamente desde la consola
- Enviar mensajes a los equipos
- Importar grupos y contenedores desde Active Directory
- Generar contraseñas de un solo uso
- Programar acciones
- Personalizar la consola Enterprise
- Actualizar la clave de licencia

La consola Enterprise solo puede reactivar un equipo desde un estado de apagado si el equipo está correctamente configurado para encenderse cuando se reciba un paquete Wake-on-LAN.

Inicio de la consola Enterprise

La consola Enterprise se instala con el Administrador de configuración de Deep Freeze. Seleccione la siguiente ruta en el menú Inicio para abrir la consola:

Inicio > *Todos los programas* > *Faronics* > *Deep Freeze Enterprise 7* > *Deep Freeze Console*

Activación de la consola Enterprise

Como función de seguridad de Deep Freeze Enterprise, la función OTP (contraseña de un solo uso) impide el uso no autorizado de la consola Deep Freeze Enterprise. Si el archivo*DFConsole.exe* se copia a un nuevo equipo, es preciso activar la consola. La primera vez que se ejecute en un equipo, se mostrará un cuadro de diálogo con un token de OTP.



El administrador de red deberá introducir este token en el sistema de generación de OTP del Administrador de configuración. Se generará una OTP. Introdúzcala en el cuadro de diálogo para que se ejecute la consola.

El equipo donde está instalada la consola Enterprise no debe tener una instalación de la semilla de estación de trabajo (con el mismo puerto) ni una instalación completa de Deep Freeze.

Iconos de Estado

La consola Enterprise muestra el estado de los equipos de la red de área local mediante los iconos siguientes, junto o sobre el nombre del equipo, en función de la vista seleccionada:

Icono	Definición
	Destino: equipos que tienen la semilla de estación de trabajo de Deep Freeze instalada, pero que no tienen instalado Deep Freeze; Deep Freeze solo puede instalarse de forma remota en los equipos con este icono.
	Equipos con Deep Freeze instalado en modo Congelado
	Equipos con Deep Freeze instalado en modo Descongelado
	Equipos con Deep Freeze instalado en modo Descongelado y bloqueado
	Equipos apagados
	Equipos en modo de mantenimiento
	Equipos cuya comunicación con la consola se ha interrumpido
	Equipos bloqueados



Ver columnas

La consola Deep Freeze Enterprise permite especificar las columnas que se muestran en el panel Estaciones de trabajo. Siga los pasos descritos a continuación para visualizar las columnas deseadas:

1. Vaya a *Ver* > *Columnas*.
2. Seleccione las siguientes columnas para visualizar:

- Configuración
- Fecha de configuración
- Fecha de caducidad
- Archivo de instalación
- Dirección IP
- Estado de la licencia
- Nombre de inicio de sesión
- Dirección MAC
- Sistema operativo
- Puerto
- Estado
- Versión
- Grupo de trabajo
- Anti-Virus



Selección basada en el estado

Puede seleccionar las estaciones de trabajo en función del estado de Deep Freeze en las estaciones de trabajo gestionadas. La selección basada en el estado puede realizarse mediante el menú *Seleccionar* en la consola Deep Freeze Enterprise. El menú Seleccionar incluye las opciones siguientes:

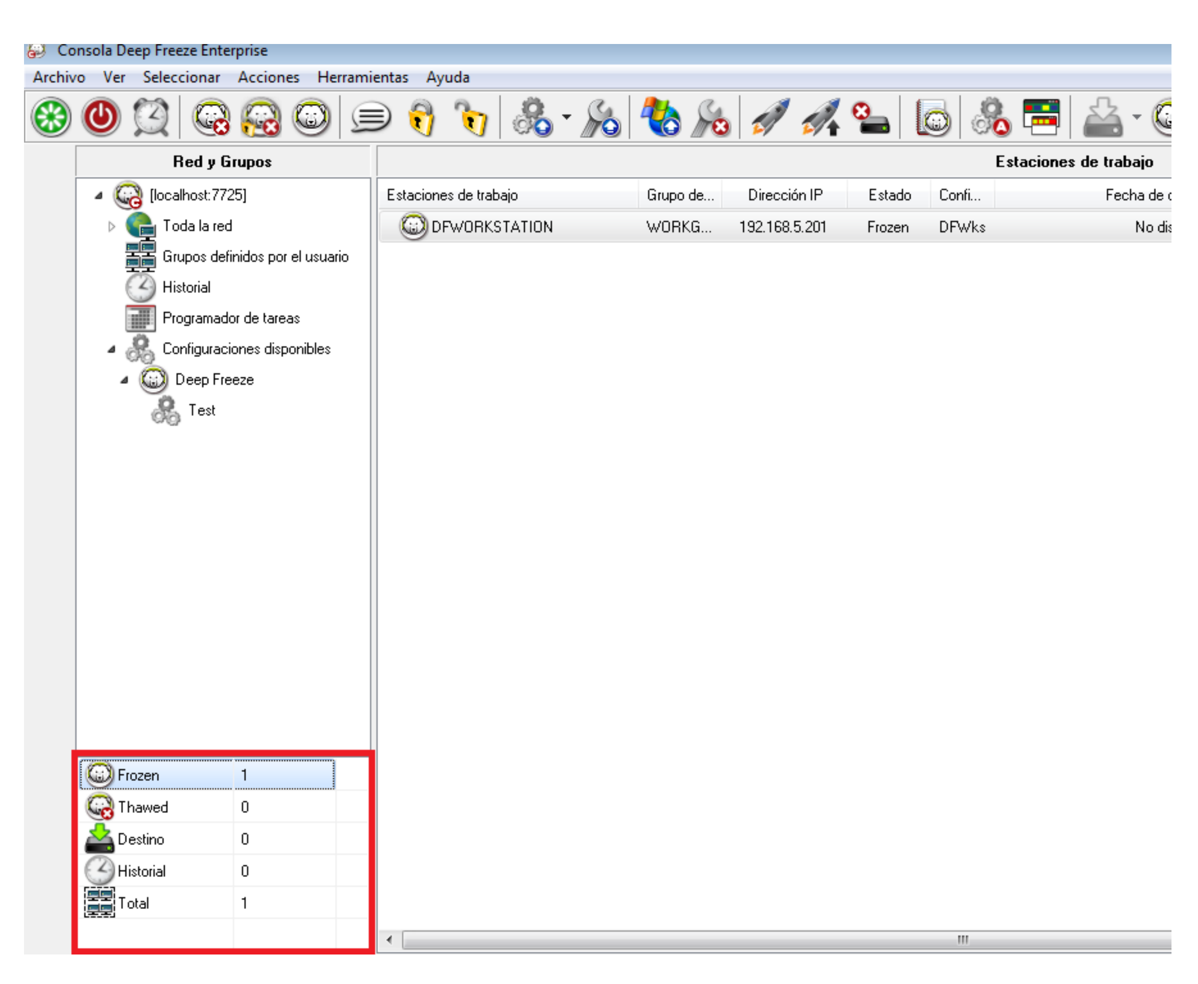
- Seleccionar todo en modo Congelado: selecciona las estaciones de trabajo en modo Congelado. También se seleccionan las estaciones de trabajo en modo Congelado y bloqueado.
- Seleccionar todo en modo Descongelado: selecciona las estaciones de trabajo en modo Descongelado. También se seleccionan las estaciones de trabajo en modo Descongelado y bloqueado.
- Seleccionar todos los destinos: selecciona todos los equipos de destino donde se puede instalar Deep Freeze.
- Seleccionar todo: selecciona todas las estaciones de trabajo.

Las siguientes opciones de selección también están disponibles en el panel Estado:

- Congelado: selecciona las estaciones de trabajo en modo Congelado. También se seleccionan las estaciones de trabajo en modo Congelado y bloqueado.
- Descongelado: selecciona las estaciones de trabajo en modo Descongelado. También se seleccionan las estaciones de trabajo en modo Descongelado y bloqueado.
- Destino: selecciona todos los equipos de destino donde se puede instalar Deep Freeze.
- Historial: muestra el historial.
- Total: selecciona todas las estaciones de trabajo.

El panel de estado de la consola Deep Freeze Enterprise también puede utilizarse para seleccionar y mostrar el número de estaciones de trabajo con un estado determinado.




Consola Deep Freeze Enterprise
Archivo Ver Seleccionar Acciones Herramientas Ayuda
Red y Grupos
Estaciones de trabajo
[localhost:7725]
Toda la red
Grupos definidos por el usuario
Historial
Programador de tareas
Configuraciones disponibles
Deep Freeze
Test
Estaciones de trabajo
Grupo de...
Dirección IP
Estado
Confi...
DFWORKSTATION
WORKG...
192.168.5.201
Frozen
DFWks
Frozen 1
Thawed 0
Destino 0
Historial 0
Total 1



Administración de la comunicación entre la consola y las estaciones de trabajo

Existen dos tipos de conexiones de consola a estación de trabajo y de consola a consola:

1. Conexiones locales: conexiones a las que solo puede acceder la consola Enterprise que aloja dichas conexiones.
2. Conexiones habilitadas para control remoto: conexiones a las que puede acceder la consola que aloja dichas conexiones y otras consolas conectadas de forma remota.



El servicio de servidor para Deep Freeze 6.5 no actualizará de forma automática el servicio de servidor para Deep Freeze 6.4 o anterior. Ambos servicios pueden instalarse en el mismo equipo, pero solo puede ejecutarse un servicio por vez.

Un equipo puede perder la comunicación con la consola debido a alguno de estos motivos:

- El equipo se ha apagado de forma manual o sin previo aviso
- La red está experimentando tráfico intenso o interrupciones del suministro eléctrico.
- La configuración de red del equipo ha cambiado para hacer referencia a una nueva consola.

En la mayoría de los casos, la comunicación con el equipo se restablece cuando el equipo se enciende o cuando se corrigen las condiciones que causaron el problema de comunicación la falla en la comunicación. Pueden pasar varios minutos antes de que el equipo conteste a la consola y se restablezca la comunicación. Si no se puede restablecer la comunicación, póngase en contacto con el *Soporte Técnico* para obtener información acerca de cómo solucionar el problema.

Configurar el servicio local

El servicio local instala y mantiene las conexiones con los equipos.

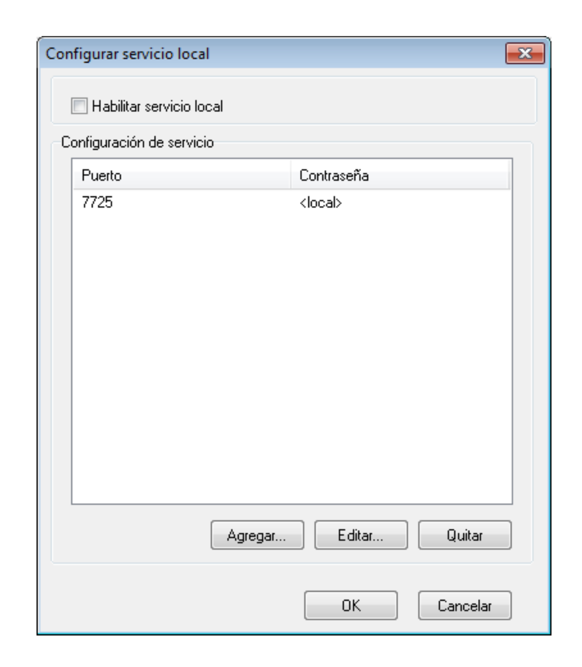
Habilitar el servicio local

El servicio local se instala y habilita de forma predeterminada la primera vez que se ejecuta la consola.

Para volver a habilitar el servicio local si se ha deshabilitado (y/o desinstalado)

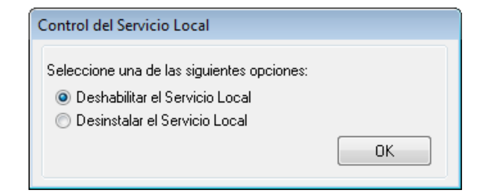
1. Seleccione *Herramientas* > *Configuración de red*.
2. Seleccione la casilla de verificación *Habilitar servicio local* para habilitarlo.





Deshabilitar el servicio local

Al desactivar la casilla de verificación *Habilitar servicio local* y hacer clic en *Aceptar* se muestra la opción para deshabilitar o desinstalar el servicio local.

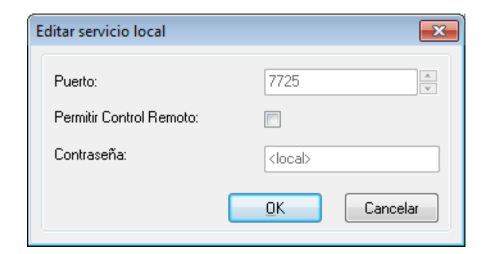


Agregar una conexión de servicio local

1. Para agregar una conexión de servicio local, seleccione *Herramientas >Configuración de red*.
2. Para agregar una conexión, seleccione Agregar y especifique el número de puerto (*7725* en este caso).
3. Para permitir que la consola pueda controlarse de forma remota, seleccione la casilla de verificación *Permitir control remoto* y especifique una contraseña.

Después de seleccionar *Agregar*, se creará una conexión para el puerto *7725* en la lista de conexiones del servicio local, así como en el panel de red de la consola.





Editar o eliminar una conexión de servicio local

Una vez se haya agregado una conexión de servicio local, puede editarse o eliminarse a través de *Herramientas > Configuración de red*.

Para editar una conexión de servicio local, siga estos pasos:

1. Asegúrese de que la opción *Habilitar servicio local* esté seleccionada.
2. Seleccione un puerto de la lista de conexiones de servicio local y haga clic en *Editar*.
3. Aparecerá el cuadro de diálogo Editar que permite que el puerto sea controlado de forma remota y protegido con contraseña.
4. Para quitar un puerto del servicio local, seleccione el puerto y haga clic en *Quitar*. Esto no eliminará la entrada del panel *Red y grupos* en la consola Enterprise. Simplemente la eliminará de la lista de conexiones de servicio local.
5. Para quitar la entrada del panel de red en la consola, selecciónela y haga clic en el icono *Quitar* en la barra lateral.



Consolas remotas

Una consola remota es una consola que aloja una o varias conexiones que permiten a otras consolas conectarse. Las conexiones existentes deben modificarse para que se pueda acceder a ellas de forma remota.

Configuración de conexiones habilitadas para control remoto

Para permitir el acceso a una conexión de forma remota, siga estos pasos:

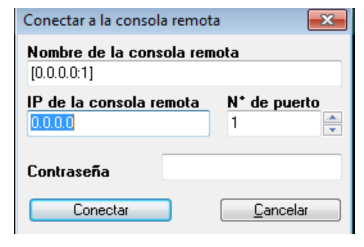
1. Abra *Herramientas* > *Configuraciones de red*.
2. Seleccione la casilla de verificación *Habilitar servicio local*.
3. Seleccione un puerto de la lista y haga clic en *Editar*.
4. Asegúrese de que la opción *Permitir control remoto* esté seleccionada.
5. Especifique una contraseña.
6. Haga clic en *Aceptar*.



Conexión con una consola remota

Una vez que la consola host haya establecido una consola remota, otras consolas pueden acceder a ella desde otro equipo.

1. Seleccione el icono *Conectar con consola remota* en la barra lateral o haga clic con el botón secundario en el elemento de la red. Al seleccionar *Conectar con consola remota*, aparecerá el cuadro de diálogo:



2. En el cuadro de diálogo *Conectar con consola remota* especifique los detalles de la conexión, como *Nombre de la consola remota*, *IP de la consola remota*, *Número de puerto,* y *Contraseña*. Esta información la proporciona el administrador de la consola host. Una vez introducida dicha información, puede recuperarse haciendo clic con el botón secundario en el panel *Red y grupos* y seleccionando *Propiedades*.



Si se corta la conexión con una consola remota, puede restablecerse la conexión haciendo clic en el icono *Volver a conectar con consola remota* en la barra lateral o haciendo clic con el botón secundario en el panel *Red y grupos*.



Gestión de Deep Freeze con la consola

La consola Enterprise contiene una barra de herramientas en la parte superior de la pantalla que ofrece un acceso rápido a las funciones de la consola.

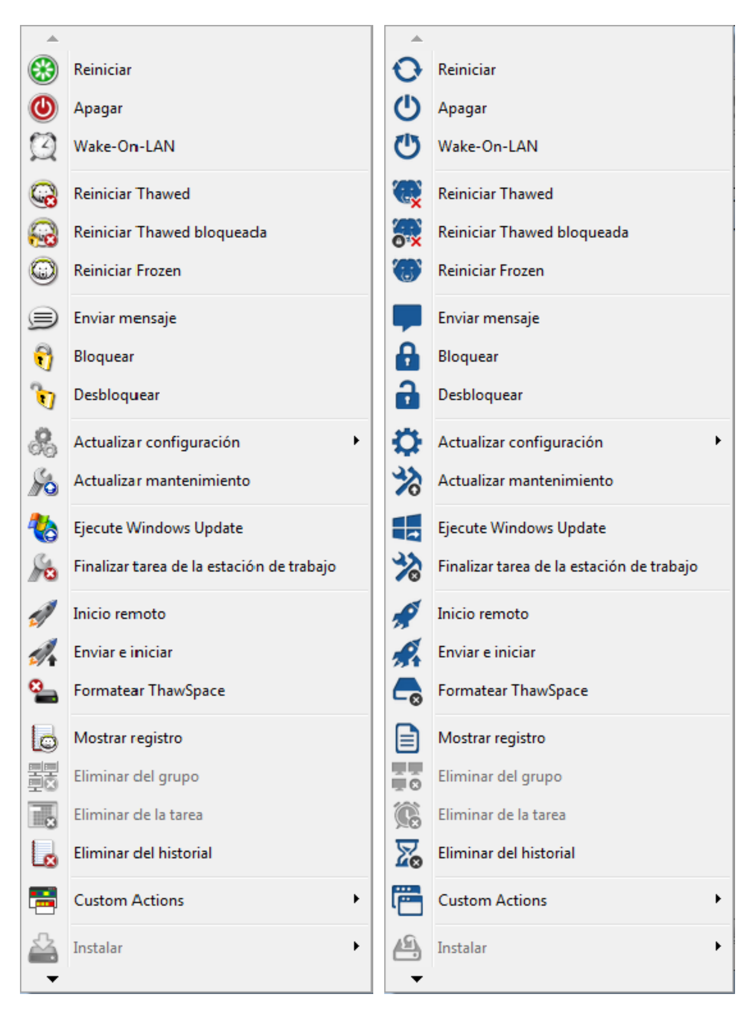
Vaya a *Ver* > *Vista clásica* para ver los iconos en el formato de Windows clásico.



Vaya a *Ver* > *Vista moderna* para ver los iconos en el formato de Windows moderno.



También se puede acceder a estos comandos desde el menú contextual, tal y como se muestra a continuación, que aparece al hacer clic con el botón secundario en uno o más equipos. Cuando se elige una acción en particular, el equipo seleccionado realiza la acción y los iconos de estado se actualizan en consecuencia. Si se seleccionan varios equipos, la acción solo se aplicará a los equipos pertinentes. Por ejemplo, si se seleccionan equipos que están en modo Descongelado y Congelado, y se aplica la acción Reiniciar como descongelado, solo los equipos en modo Congelado se reiniciarán en modo Descongelado. La acción no se aplicará a los equipos que ya estén en modo Descongelado.





Algunos iconos específicos aparecen como desactivados si el equipo seleccionado no admite dicha acción. Por ejemplo, un equipo con un icono *Destino* no mostrará las opciones correspondientes a poner en modo Descongelado o Congelado, porque todavía no se ha instalado el programa.

Actualización del software Deep Freeze

Para actualizar los equipos Deep Freeze (en los que está instalado Deep Freeze 7.7 o posterior) con una nueva versión de Deep Freeze, siga estos pasos:

1. En la consola Enterprise, seleccione los equipos que se van a actualizar. Los equipos pueden estar en modo Congelado o Descongelado.
2. Haga clic con el botón secundario y seleccione *Actualizar Deep Freeze* en el menú contextual.
3. Los equipos seleccionado se actualizarán a la nueva versión del software Deep Freeze, pero conservarán todos los ajustes de la versión actual. Los equipos se reiniciarán dos veces para completar la actualización.

Envío de mensajes a equipos

Para enviar un mensaje a uno o más equipos, siga estos pasos:

1. Seleccione los equipos a los que se enviará un mensaje.
2. Haga clic con el botón secundario y seleccione *Enviar mensaje* en el menú contextual.
3. Escriba el mensaje en el cuadro de diálogo que aparece y haga clic en *Enviar*. Aparecerá un cuadro de diálogo que solicitará una confirmación para enviar el mensaje a los equipos seleccionados.
4. Haga clic en *Aceptar*para enviar o en *Cancelar* para cerrar el cuadro de diálogo sin enviar el mensaje.

Instalación localizada de Deep Freeze

Siga estos pasos para instalar de forma remota una instalación de estación de trabajo completa en cualquier equipo que tenga instalada la semilla de estación de trabajo.

1. Haga clic con el botón secundario en uno o varios equipos y seleccione *Instalar*. Aparecerá un cuadro de diálogo que le pedirá confirmación para proseguir con la instalación. Haga clic en *Aceptar*.
2. Aparecerá un cuadro de diálogo para que seleccione el archivo que se va a instalar en el equipo remoto.
3. Seleccione el archivo de instalación y haga clic en *Abrir*.
4. El equipo instalará Deep Freeze y se reiniciará.
5. Una vez finalizada la instalación, la consola Enterprise reflejará el cambio en el estado del equipo y lo mostrará como *Congelado*.

Actualización de un archivo de configuración de Deep Freeze

Siga estos pasos para actualizar la configuración de uno o más equipos con los ajustes de un archivo *.rdx* existente. (Un archivo *.rdx* contiene las condiciones especificadas en el Administrador de configuración de Deep Freeze).



1. Haga clic con el botón secundario en los equipos y seleccione *Actualizar con archivo RDX*.
2. Aparecerá un mensaje que le solicitará ubicar un archivo *.rdx* existente.
3. Haga clic en *Aceptar*. Aparecerá un cuadro de diálogo estándar *Abrir archivo* para seleccionar un archivo *.rdx* .
4. Busque un archivo y haga clic en *Abrir* para actualizar la configuración en los equipos seleccionados con los ajustes del archivo *.rdx*. Haga clic en *Cancelar* para cancelar la actualización de la configuración.

Ejecutar actualizaciones de Windows

Las actualizaciones de Windows pueden aplicarse a petición desde el menú contextual al que se accede al hacer clic con el botón secundario.

Siga los pasos descritos a continuación para ejecutar las actualizaciones de Windows en la estación de trabajo.

1. Haga clic con el botón secundario en los equipos y seleccione *Ejecutar actualización de Windows*.
2. Haga clic en *Aceptar*.

Las actualizaciones de Windows se aplicarán a las estaciones de trabajo seleccionadas. Se usarán los ajustes configurados en la *Ficha Actualización de Windows*.

Además de aplicar las actualizaciones de Windows a petición desde el menú contextual al que se accede al hacer clic con el botón secundario, también puede programar las tareas de actualización de Windows. Para más información, consulte *Programación de tareas de Deep Freeze* acerca de cómo programar una tarea de actualización de Windows.



Si las opciones de red de la nueva configuración han cambiado, es posible que los equipos pierdan la comunicación con la consola Enterprise existente. Si se pierde la comunicación con los equipos, verifique los ajustes de red de los equipos actualizados para asegurarse de que los números de puerto y/o la dirección IP de la consola no hayan cambiado.



Los cambios de contraseña surten efecto de inmediato. Todos los demás cambios surtirán efecto después de reiniciar cada equipo. No es posible modificar los ThawSpaces y/o las unidades en modo Congelado mediante la actualización del archivo de configuración.

Formatear ThawSpace

La consola Deep Freeze Enterprise permite formatear todos los ThawSpaces de forma remota en las estaciones de trabajo gestionadas.

Siga los pasos descritos a continuación para formatear ThawSpaces:

1. Seleccione una o varias estaciones de trabajo.
2. Haga clic con el botón secundario para seleccionar Formatear ThawSpace. También puede hacer clic en el icono Formatear ThawSpace en la barra de herramientas.
3. Se mostrará la advertencia *Se formatearán todos los ThawSpaces en los equipos seleccionados.*
4. *¿Desea continuar?*.





5. Haga clic en *Aceptar*.



El comando Formatear ThawSpaces elimina todos los datos en los ThawSpaces. Los datos no podrán recuperarse una vez eliminados. Realice una copia de seguridad de los archivos importantes antes de formatear un ThawSpace.



Licencia

La clave de licencia puede actualizarse a través de la consola Enterprise.

Para actualizar la clave de licencia, siga estos pasos:

1. Inicie la *consola Enterprise*.
2. Vaya a *Herramientas* > *Licencia*.
3. Se mostrará el cuadro de diálogo *Licencia de Deep Freeze*.



4. Haga clic en *Editar* e introduzca la clave de licencia en el campo *Clave de licencia*.
5. Haga clic en *Actualizar licencia*. Deep Freeze pasará de ser una versión de *Evaluación* a una versión *Con licencia*. El campo *Tipo de clave de licencia* muestra la *Clave de licencia*. El campo *Fecha de caducidad* muestra la fecha y la hora en las que vence la licencia.
6. Haga clic en *Activar en línea* para activar la licencia de Deep Freeze a través de Internet. El equipo debe estar conectado a Internet para poder realizar la activación en línea. La licencia de Deep Freeze se debe activar dentro de los 30 días siguientes a la instalación o Deep Freeze dejará de funcionar. Durante la activación, Faronics autenticará la licencia de Deep Freeze.
7. Como alternativa, haga clic en *Opciones de activación*. Hay dos opciones disponibles:





- Seleccione *Activar en línea* para activar la licencia de Deep Freeze en línea. Esta opción es igual que la del paso 1. Haga clic en *Siguiente* después de seleccionar esta opción. Deep Freeze se activará en línea al hacer clic en *Siguiente*.
- Seleccione *Activar sin conexión*. Esta opción permite realizar la activación por teléfono o correo electrónico. Haga clic en *Siguiente* después de activar. Aparecerá la pantalla Activar sin conexión.

8. Proporcione los *Detalles de activación* al Servicio de activación de Faronics por teléfono o correo electrónico. Una vez que reciba el código de activación de Faronics, introdúzcalo en el campo *Código de activación* y haga clic en *Siguiente*. Ahora la licencia de Deep Freeze está activada.



La clave de licencia se actualiza automáticamente en todos los equipos que se comunican con la consola Enterprise. Si un equipo está desconectado (apagado o desconectado de la red), la clave de licencia se actualizará la próxima vez que el equipo se comunique con la consola Enterprise.



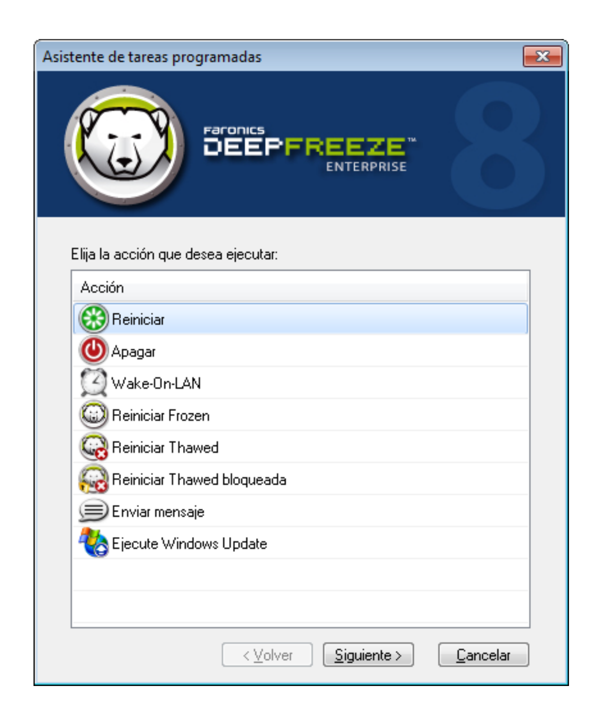
Programación de tareas de Deep Freeze

Para programar una tarea de Deep Freeze en la consola Enterprise utilizando el Asistente para tareas programadas, complete los siguientes pasos:

1. Abra el *Asistente para tareas programadas* de una de las siguientes maneras:

- haga clic en *Programador* en el panel *Red y grupos* y haga clic en el icono *Agregar tarea*.
- haga clic con el botón secundario en *Programador* en el panel *Red y grupos* y seleccione *Agregar tarea*.

Se mostrará la pantalla siguiente:



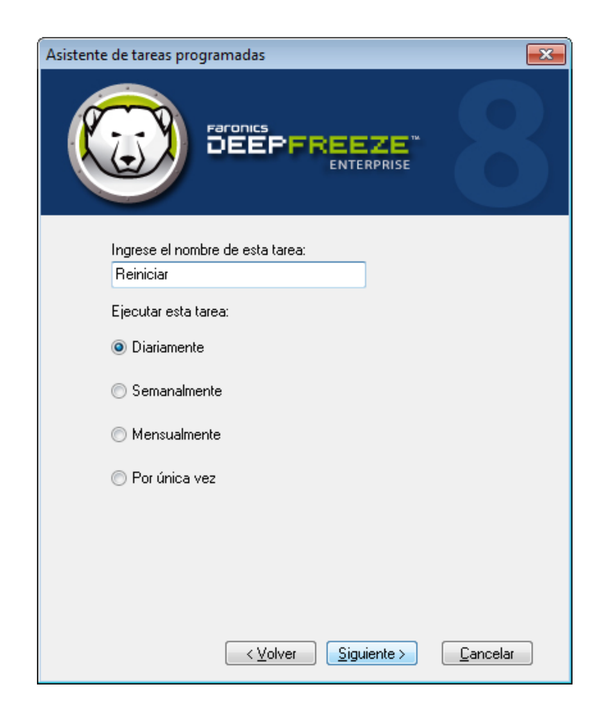
2. Haga doble clic en la tarea deseada o seleccione la tarea y haga clic en *Siguiente*. Las siguientes tareas están disponibles para Deep Freeze:

- Reiniciar
- Apagar
- Wake-On-LAN
- Reiniciar como congelado
- Reiniciar como descongelado
- Reiniciar como descongelado y bloqueado
- Enviar mensaje
- Ejecutar actualizaciones de Windows

3. En la siguiente pantalla, introduzca el nombre de la tarea y seleccione la programación de ejecución de la tarea: Diariamente, Semanalmente, Mensualmente o Solo una vez. Los



nombres de tarea deben ser únicos. Dos tareas no pueden tener el mismo nombre. Haga clic en *Siguiente*.

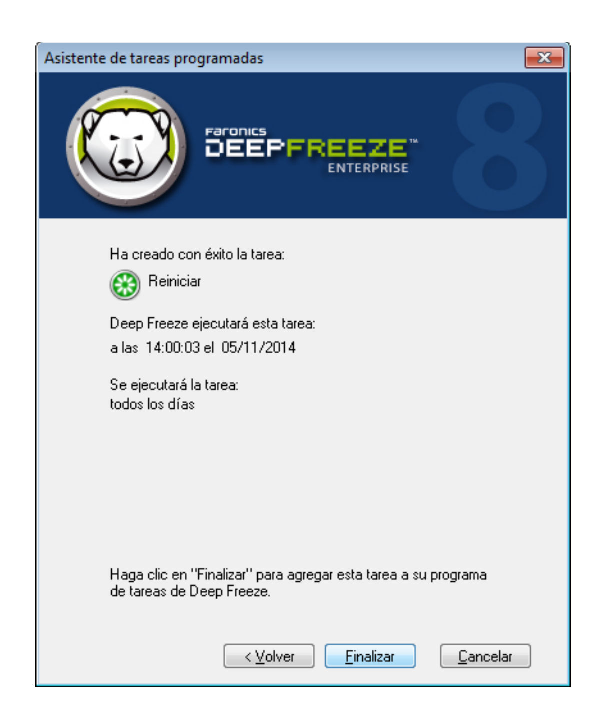


4. Las opciones de configuración de fecha y hora pueden variar en función de los ajustes especificados para la ejecución de la tarea. Haga clic en *Siguiente*.



5. Haga clic en *Finalizar* una vez completada la configuración.





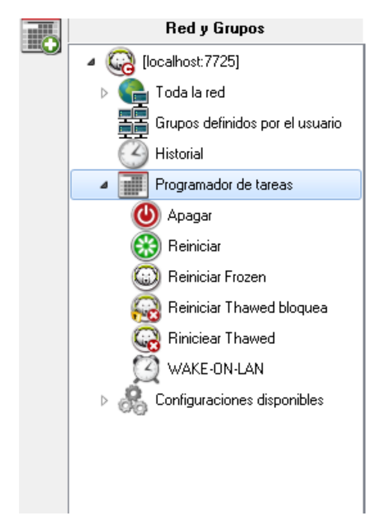


La hora de inicio predeterminada de una tarea es cinco minutos a partir de la hora actual.



Asignación de equipos a tareas programadas

Una vez programada una tarea, aparecerá en *Programador*, en el panel *Red y grupos* de la consola.



Para asignar equipos a una tarea, seleccione los equipos deseados en el panel *Estaciones de trabajo* de la consola y arrástrelos a la tarea deseada. O arrastre un grupo a la tarea.

Para ver qué equipos están asignados a una tarea específica, haga clic en la tarea. Los equipos asignados se mostrarán en el panel *Estaciones de trabajo*.

Para eliminar un equipo de una tarea, haga clic en el equipo y pulse *Eliminar*.

Para eliminar un equipo de una tarea, haga clic con el botón secundario en el equipo y seleccione *Eliminar de tarea*.



Ejecución de una tarea de forma inmediata

Para ejecutar una tarea de forma inmediata, haga clic con el botón secundario en la tarea y seleccione *Ejecutar tarea*.

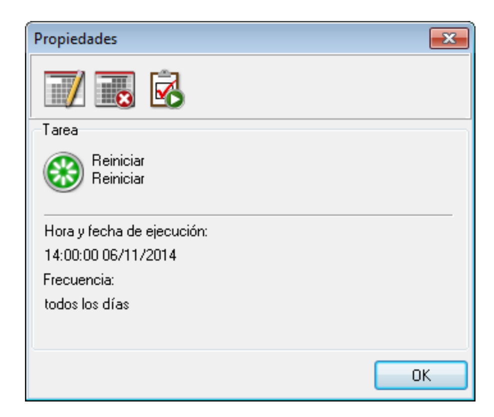
Eliminación de una tarea

Para eliminar una tarea, haga clic en la tarea y pulse *Eliminar*.

Propiedades de las tareas programadas

Para ver las propiedades de una tarea, haga clic con el botón secundario en el nombre de la tarea y seleccione *Ver propiedades*.

Aparecerá la siguiente pantalla:



Una vez creada una tarea, no es posible modificar sus propiedades. Solo se pueden modificar los equipos que ejecutarán la tarea agregando o eliminando equipos.



Las tareas programadas se ejecutarán aunque la consola Enterprise esté cerrada siempre que el servicio local esté habilitado y las conexiones de red no estén desactivadas al salir de la consola Enterprise.



Administración de red y grupos

La consola Enterprise organiza los equipos automáticamente por grupo de trabajo o dominio. Haga clic en el grupo de trabajo o dominio correspondiente para visualizar los equipos de dicho grupo de trabajo o dominio.

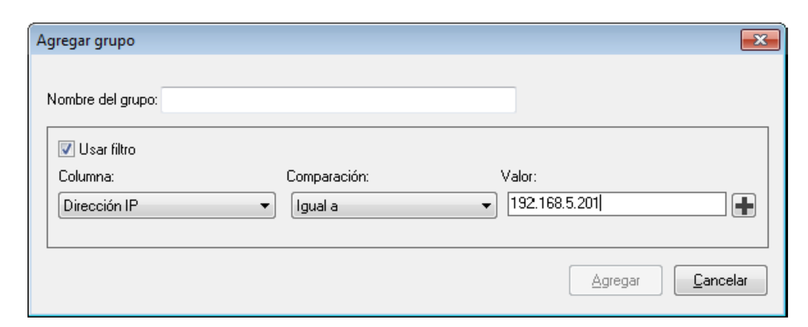
La consola Enterprise también puede utilizarse para definir grupos específicos que permitan organizar los equipos.

Agregar un grupo

El cuadro de diálogo Agregar grupo permite configurar varios filtros para ordenar las estaciones de trabajo en varios grupos. Este filtro actualiza automáticamente la lista de estaciones de trabajo en función de los cambios en los parámetros seleccionados.

Siga los pasos descritos a continuación para agregar un grupo con un filtro:

1. Haga clic con el botón secundario en *Grupos definidos por el usuario* en el panel *Red y grupos*.
2. Seleccione *Agregar grupo*. Se mostrará el cuadro de diálogo Agregar grupo:



3. Especifique el *Nombre de grupo*.
4. Seleccione *Columna*.
5. Seleccione *Comparación*.
6. Seleccione *Opción* Y/O si desea agregar otro filtro.
7. Especifique *Valor* o *Expresión regular*.
8. Haga clic en *Agregar*.

La siguiente tabla muestra la columna, la comparación, la opción y los valores.

Seleccionar Columna	Seleccionar Comparación	Seleccionar Opción	Especificar Valor o Expresión regular
Estaciones de trabajo	Igual a Distinto de Expresión regular	Y O	Especifique el *Valor* o la *Expresión regular*.



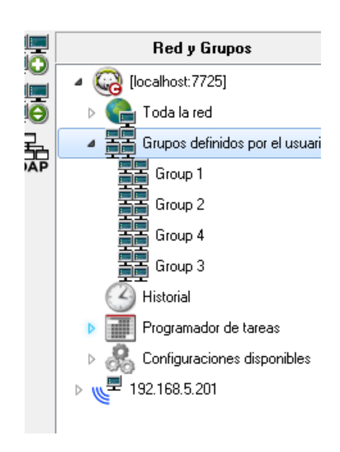
Seleccionar Columna	Seleccionar Comparación	Seleccionar Opción	Especificar Valor o Expresión regular
Grupo de trabajo	Igual a Distinto de Expresión regular	Y O	Especifique el *Valor* o la *Expresión regular*.
Dirección IP	Igual a Mayor que Mayor o igual que Menor que Menor o igual que Expresión regular	Y O	Especifique el *Valor* o la *Expresión regular*.
Estado	Igual a Distinto de Expresión regular	Y O	Congelado Congelado y bloqueado Descongelado Descongelado y bloqueado Aplicando actualización de Windows Aplicando Archivo por lotes Periodo de descongelación Modo de mantenimiento Licencia caducada Semilla de estación de trabajo Desconocido
Configuración	Igual a Distinto de Expresión regular	Y O	Especifique el *Valor* o la *Expresión regular*.
Fecha de configuración	Igual a Mayor que Mayor o igual que Menor que Menor o igual que Expresión regular	Y O	Especifique la *Fecha*.



Seleccionar Columna	Seleccionar Comparación	Seleccionar Opción	Especificar Valor o Expresión regular
Archivo de instalación	Igual a Distinto de Expresión regular	Y O	Especifique el *Valor* o la *Expresión regular*.
Versión	Igual a Mayor que Mayor o igual que Menor que Menor o igual que Expresión regular	Y O	Especifique el *Valor* o la *Expresión regular*.
Sistema operativo	Igual a Distinto de Expresión regular	Y O	Especifique el *Valor* o la *Expresión regular*.
Dirección MAC	Igual a Distinto de Expresión regular	Y O	Especifique el *Valor* o la *Expresión regular*.
Nombre de inicio de sesión	Igual a Distinto de Expresión regular	Y O	Especifique el *Valor* o la *Expresión regular*.

Construcción de una estructura de grupo definida por el usuario

Una vez que se agrega un grupo, se pueden añadir uno o varios subgrupos debajo de forma indefinida como una forma de diferenciar los entornos, como se muestra en el ejemplo siguiente:

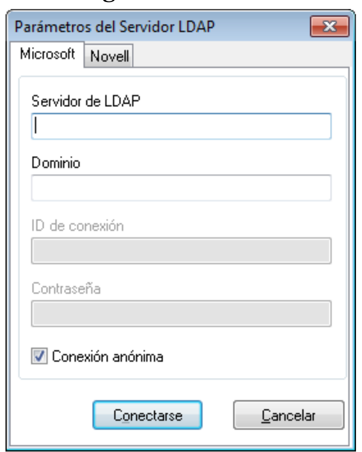




Importación de grupos desde Active Directory

Si la estructura de grupo se ha diseñado en Active Directory, puede importarse directamente en la consola Enterprise. Siga estos pasos para importar desde Active Directory:

1. Seleccione *Herramientas> Importar grupos desde Active Directory* o haga clic en el icono *LDAP* en la barra lateral.
2. Aparecerá el siguiente cuadro de diálogo: Seleccione la ficha *Microsoft* o la ficha *Novell*.



3. Introduzca la información del servidor LDAP correspondiente a la ubicación de la importación. La opción de inicio de sesión anónima también está disponible. Si esta casilla de verificación no está seleccionada, se requerirá un nombre de usuario y una contraseña.
4. Haga clic en *Conectar*. Aparecerá a jerarquía de *Active Directory*. Seleccione las entradas y haga clic en *Importar*



Historial

La consola Enterprise almacena el historial de los equipos de destino.

Si un equipo se desconecta de una red, se apaga o se reinicia, aparecerá un signo de exclamación (!) en la consola Enterprise para ese equipo en particular. Si el equipo se vuelve a conectar, el signo de exclamación desaparece.

Si el equipo se desconecta de forma permanente (por ejemplo, si el equipo se desconecta de forma permanente de la red) o si el equipo se apaga, el signo de exclamación permanece visible.

En la consola Enterprise, vaya a *Archivo > Salir*. Seleccione la opción *Cerrar consola Deep Freeze y cerrar las conexiones de red* y haga clic en *Aceptar*. Cuando vuelva a abrir la consola Enterprise, los equipos con el signo de exclamación (!) aparecerán en el Historial. Si el equipo está apagado y cuenta con el hardware Wake-On-LAN, haga clic con el botón secundario en Historial en el equipo y seleccione Wake-On-LAN para reactivar el equipo.

Opciones en el Historial:

- Para ver el historial haga clic en *Historial* en el panel *Red y grupos*.
- Para eliminar equipos del historial, selecciónelos, haga clic con el botón secundario y seleccione *Quitar del historial* en el menú contextual.
- Para activar el equipo con Wake-On-LAN, seleccione los equipos, haga clic con el botón secundario y seleccione *Wake-ON-LAN* en el menú contextual.



Agregar equipos a un grupo

Se pueden agregar equipos a un grupo arrastrándolos desde el panel *Estaciones de trabajo* hasta el grupo deseado o utilizando un filtro automático establecido durante la creación de los grupos.

El filtrado de grupos automático permite agregar equipos de forma automática a grupos definidos por el usuario. Los equipos se agregan según el nombre de equipo.

Se pueden utilizar comodines (*, ?) para agregar un grupo de equipos basado en un segmento específico del nombre.

Ejemplo: *Lab1-** agrega todas los equipos cuyos nombres comienzan con Lab1-.

Clasificación alfabética de grupos

Para clasificar los grupos en orden alfabético, haga clic con el botón secundario en *Grupos definidos por el usuario* y seleccione *Ordenar grupos alfabéticamente*.

Eliminación de estaciones de trabajo de un grupo definido por el usuario

Para eliminar un equipo de un grupo, haga clic con el botón secundario en el equipo en *Grupos definidos por el usuario* y seleccione *Eliminar del grupo*.

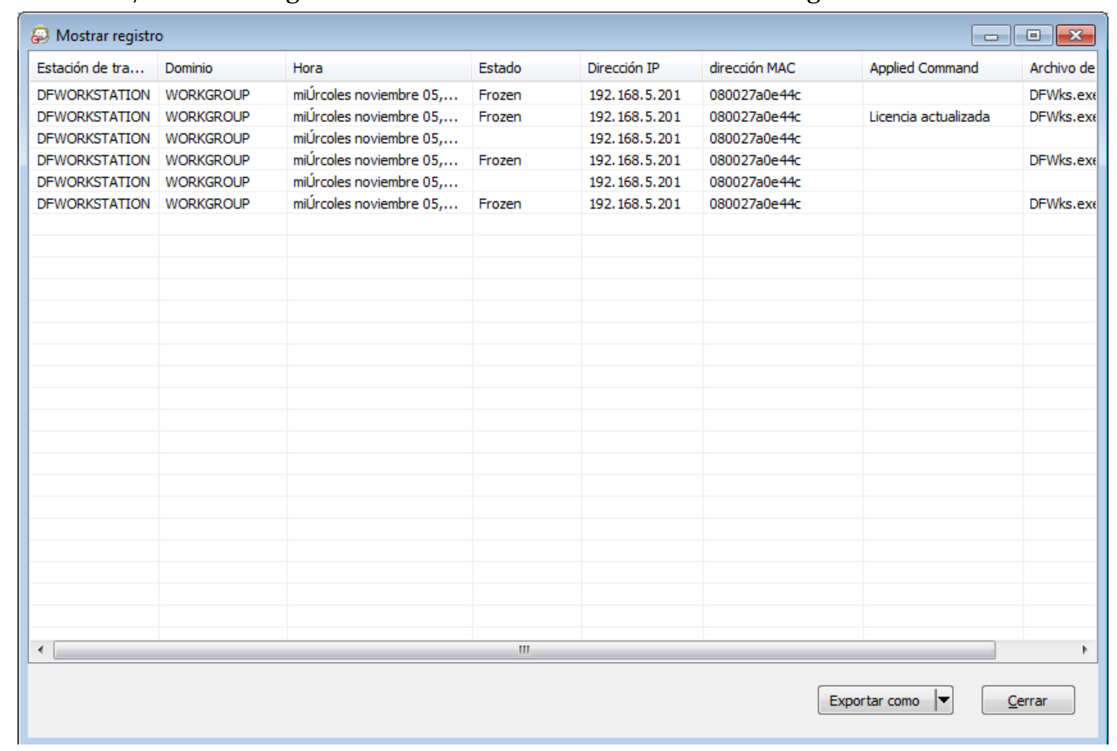
Importación o exportación de grupos a un archivo

Para importar grupos desde un archivo o exportar grupos a un archivo, seleccione la opción deseada en el menú *Herramientas*.



Acceso al archivo de registro de la consola

La consola Enterprise lleva un registro del estado y del historial de actividad de todas los equipos conectados. El registro únicamente almacena información de los últimos 7 días. Toda información con más de 7 días de antigüedad se eliminará automáticamente del registro.



- Para ver el archivo de registro para uno o varios equipos, haga clic con el botón secundario en los equipos y seleccione *Mostrar registro*.
- Para ordenar el archivo de registro, haga clic en el encabezado deseado. Columnas disponibles:
  - — Estación de trabajo
  - — Dominio
  - — Hora
  - — Estado
  - — Dirección IP
  - — Dirección MAC
  - — Comando aplicado (Congelado, Descongelado, Reiniciar, Apagar)
  - — Archivo de instalación
- Para exportar el archivo de registro, haga clic en Exportar como y seleccione Texto o CSV. Especifique el nombre del archivo y haga clic en Aceptar.

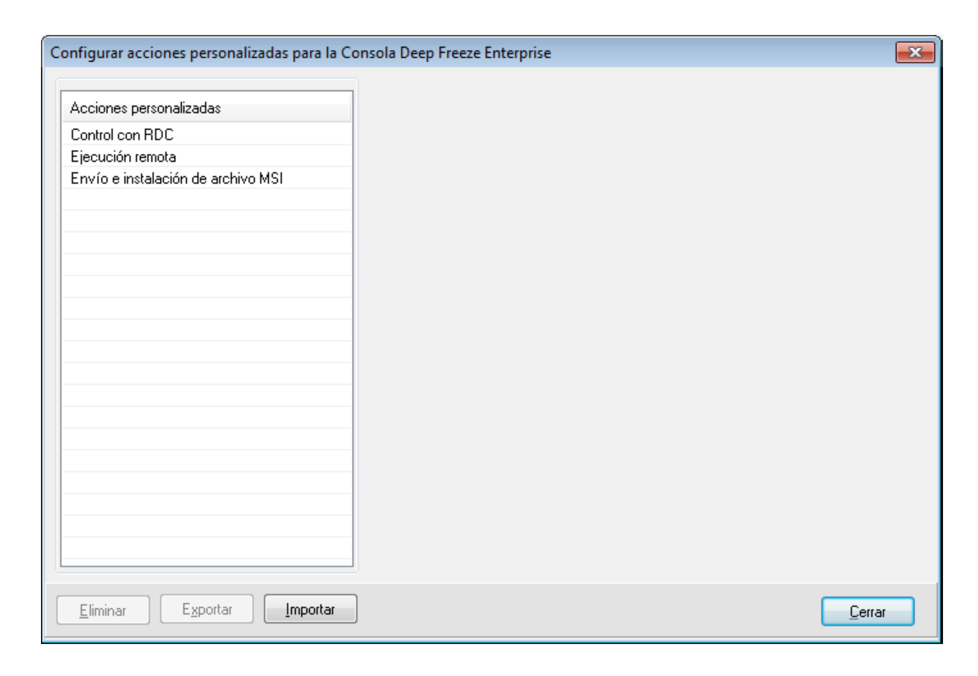


Configuración de acciones personalizadas

Deep Freeze ofrece las siguientes acciones personalizadas a las que se puede acceder a través del menú *Acciones*. Se pueden crear acciones adicionales conforme a necesidades específicas. Deep Freeze proporciona tres acciones predeterminadas. Es posible configurar acciones personalizadas adicionales importando el archivo *.xml* apropiado en la consola Deep Freeze. Para obtener más información acerca de las acciones personalizadas, la estructura del archivo de acciones personalizadas y otros parámetros, consulte *Apéndice E*.

Controlar con RDC

Permite la conexión con el equipo a través del protocolo de escritorio remoto de Microsoft. La conexión de escritorio remoto debe estar habilitada en los equipos de destino.

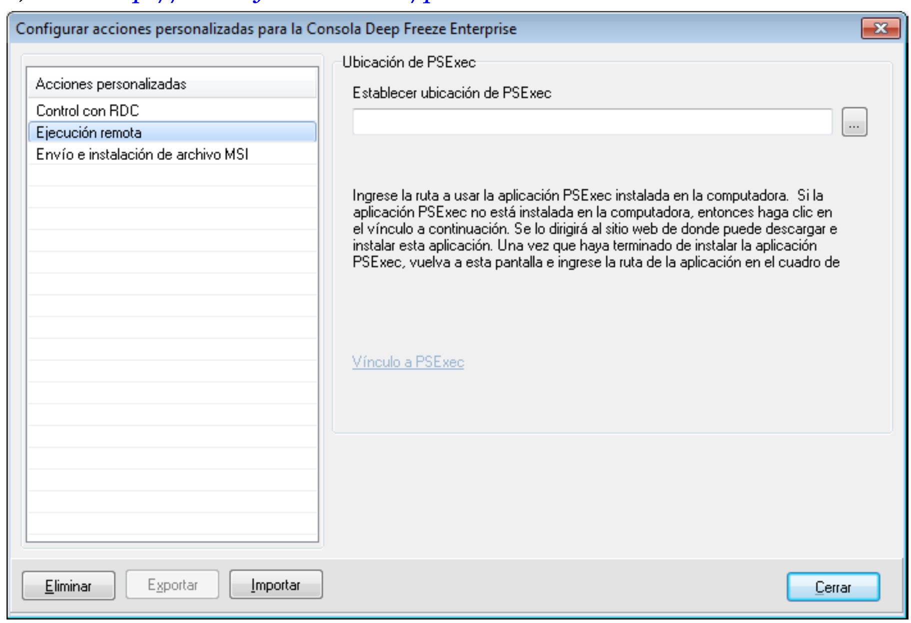


1. Vaya al menú *Acción* > *Acciones personalizadas*.
2. Seleccione *Controlar con RDC*.
3. Introduzca la *Ruta ejecutable* o busque y seleccione la ubicación.
4. Introduzca el *Directorio de trabajo*.
5. Haga clic en *Aplicar*.



Ejecución remota

La ejecución remota permite ejecutar de forma remota un archivo ejecutable en un equipo. PsExec es una herramienta que puede utilizarse para ejecutar de manera remota un archivo ejecutable en un equipo. PsExec debe descargarse e instalarse en el equipo. Para obtener más información sobre PsExec, visite *http://www.faronics.com/pstools*.



Configurar

1. Vaya a *Acción* > *Acciones personalizadas*.
2. Seleccione *Ejecución remota*.
3. Introduzca la *Ubicación de PSExec* o busque y seleccione la ubicación.
4. La *Ruta ejecutable* y el *Directorio de trabajo* se agregarán automáticamente. La *Ruta ejecutable* y el *Directorio de trabajo* pueden modificarse más tarde.
5. Haga clic en *Cerrar*.

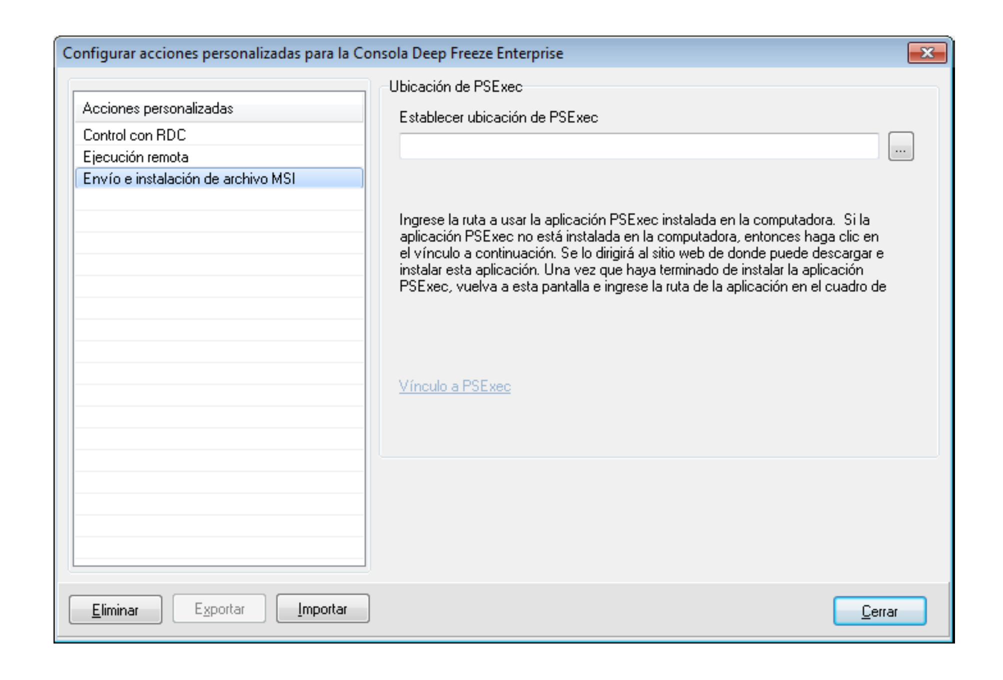
Ejecutar

1. Seleccione los equipos en el panel *Estaciones de trabajo*.
2. Seleccione *Acción* > *Ejecución remota*.
3. Se mostrará el cuadro de diálogo *Ejecución remota*.
4. Introduzca el *Nombre* de usuario, la *Contraseña* y el *Comando*.
5. Haga clic en *Aceptar*.



Enviar e instalar archivo MSI

La opción *Enviar e instalar archivo MSI* permite enviar e instalar un archivo *.msi* en un equipo a través de la consola Enterprise.



Configurar

1. Vaya a *Acción* > *Acciones personalizadas*.
2. Seleccione *Enviar e instalar archivo MSI*.
3. Introduzca la *Ubicación de PSExec* o busque y seleccione la ubicación.
4. La *Ruta ejecutable* y el *Directorio de trabajo* se agregarán automáticamente. La *Ruta ejecutable* y el *Directorio de trabajo* pueden modificarse más tarde.
5. Haga clic en *Cerrar*.

Ejecutar

1. Seleccione los equipos en el panel *Estaciones de trabajo*.
2. Seleccione*Acción*> *Enviar e instalar archivo MSI*.
3. Aparecerá el cuadro de diálogo *Enviar e instalar archivo MSI* .
4. Introduzca el *Nombre de usuario*, la *Contraseña*, el *Nombre de archivo* y la *Letra de la unidad*.
5. Haga clic en Aceptar.

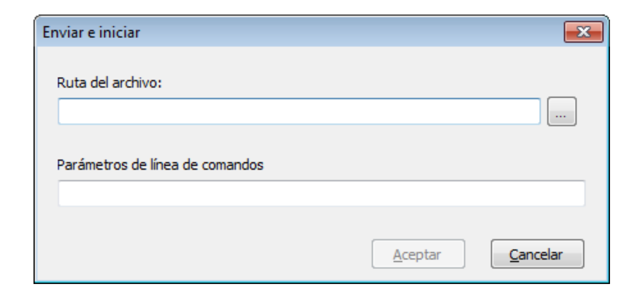
Enviar e iniciar

Puede enviar e iniciar archivos en las estaciones de trabajo gestionadas.



Siga los pasos descritos a continuación para enviar e iniciar archivos en las estaciones de trabajo gestionadas:

1. Seleccione una o más estaciones de trabajo en el panel Estación de trabajo.
2. Haga clic con el botón secundario y seleccione *Acciones* > *Enviar y ejecutar*. Se mostrará el cuadro de diálogo Enviar e iniciar:



3. Seleccione la ruta del archivo o especifíquela.

- *Nombre y ruta de archivo*: especifique el nombre y la ruta de archivo donde está ubicado el archivo en el equipo con la consola. También puede buscar y seleccionar el archivo ejecutable. Los tipos de archivo admitidos son .exe (ejecutables) y .msi (instaladores MSI). Los archivos MSI se ejecutan en modo de instalación de forma predeterminada. Por ejemplo, si el archivo ejecutable MyApplication.exe está ubicado en C:/AppFolder, especifique *C:/AppFolder/MyApplication.exe*.

4. Especifique los parámetros de la línea de comandos con variables de entorno (opcional):

- *Argumentos*: especifique los argumentos que desee aplicar con el archivo ejecutable. Por ejemplo, si el archivo ejecutable se va a ejecutar desde el símbolo del sistema con el comando C:/AppFolder/MyApplication -o logFile.log, especifique *-o logFile.log* como argumento. Para archivos .msi, especifique los argumentos que normalmente especificaría al iniciar el archivo .msi con MSIEXEC. Si no especifica ningún argumento para un archivo .msi, Deep Freeze agregará automáticamente "/i" (install) de forma automática. Deep Freeze también reemplazará cualquier opción de visualización con /qn (quiet, sin interfaz de usuario).

5. Haga clic en Aceptar.

El archivo se enviará a la estación de trabajo seleccionada y se iniciará de forma remota en las estaciones de trabajo seleccionadas.

Inicio remoto

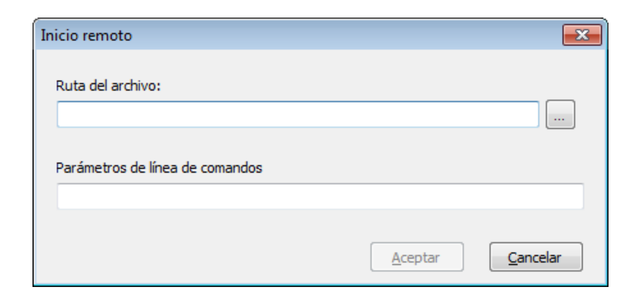
Puede iniciar de forma remota archivos en las estaciones de trabajo gestionadas.

Siga los pasos descritos a continuación para ejecutar archivos de forma remota en las estaciones de trabajo gestionadas:

1. Seleccione una o más estaciones de trabajo en el panel Estación de trabajo.



2. Haga clic con el botón secundario y seleccione *Acciones* > *Ejecución remota*. Se mostrará el cuadro de diálogo Ejecución remota:



3. Seleccione la ruta del archivo o especifíquela.

- *Nombre y ruta de archivo*: especifique el nombre y la ruta de archivo donde está ubicado el archivo en el equipo con la consola. También puede buscar y seleccionar el archivo ejecutable. Los tipos de archivo admitidos son .exe (ejecutables) y .msi (instaladores MSI). Los instaladores MSI se ejecutan en modo de instalación de forma predeterminada. Por ejemplo, si el archivo ejecutable MyApplication.exe está ubicado en C:/AppFolder, especifique *C:/AppFolder/MyApplication.exe*.

4. Especifique los parámetros de la línea de comandos con variables de entorno (opcional):

- *Argumentos*: especifique los argumentos que desee aplicar con el archivo ejecutable. Por ejemplo, si el archivo ejecutable se va a ejecutar desde el símbolo del sistema con el comando C:/AppFolder/MyApplication -o logFile.log, especifique *-o logFile.log* como argumento. Para archivos .msi, especifique los argumentos que normalmente especificaría al iniciar el archivo .msi con MSIEXEC. Si no especifica ningún argumento para un archivo .msi, Deep Freeze agregará automáticamente "/i" (install) de forma automática. Deep Freeze también reemplazará cualquier opción de visualización con /qn (quiet, sin interfaz de usuario).

5. Haga clic en Aceptar.

El archivo se ejecutará de forma remota en las estaciones de trabajo seleccionadas.

Eliminación, importación y exportación de acciones personalizadas

Eliminación de acciones personalizadas

Para eliminar acciones personalizadas, siga estos pasos:

1. Vaya al menú *Acción* > *Acciones personalizadas*.
2. Seleccione la acción personalizada que desea eliminar.
3. Haga clic en *Eliminar*.

Importación de acciones personalizadas

Para importar acciones personalizadas, siga estos pasos:

1. Vaya al menú *Acción* > *Acciones personalizadas*.
2. Haga clic en *Importar*.



3. Busque y seleccione el archivo *.xml* que se va a importar.
4. Haga clic en *Abrir* para importar el archivo.

Exportación de acciones personalizadas

Para exportar acciones personalizadas, siga estos pasos:

1. Vaya al menú *Acción* > *Acciones personalizadas*.
2. Seleccione la acción personalizada que desea exportar.
3. Haga clic en *Exportar*.
4. Se mostrará el cuadro de diálogo de Exportar acción personalizada a archivo.
5. Especifique un *Nombre de archivo* y haga clic en*Guardar*.



Personalizador de la consola

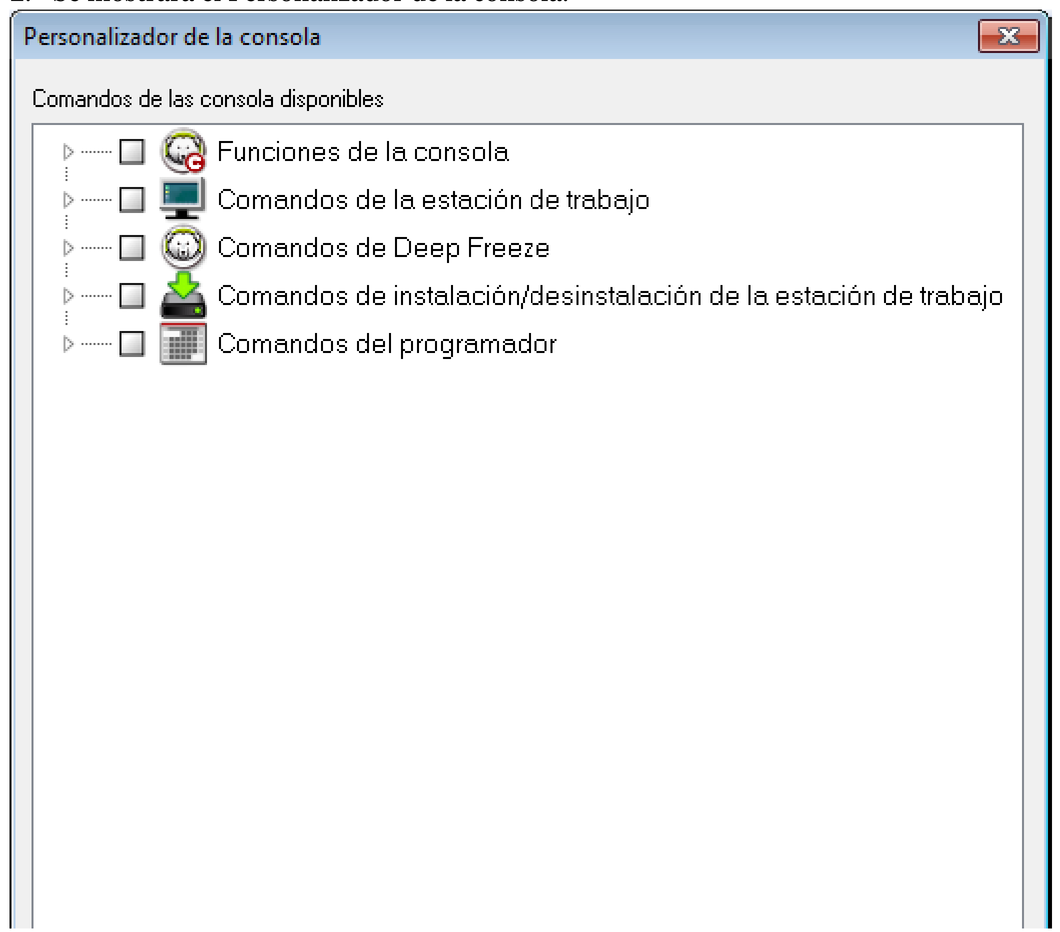
El Personalizador de la consola permite especificar qué funciones y comandos desea que estén disponibles en la consola y guardar el resultado como una nueva consola que puede distribuir en su organización.

Los ajustes disponibles se agrupan en categorías (funciones de la consola, comandos de estación de trabajo, comandos de Deep Freeze, comandos de instalación/desinstalación de estaciones de trabajo y comandos del Programador). Haga clic en el signo más (+) en el extremo izquierdo de cada categoría para obtener una lista completa de los ajustes disponibles en esa categoría.

Active o desactive las casillas de verificación individuales según sea necesario. También puede activar o desactivar todas las categorías juntas. Los ajustes desactivados no estarán disponibles en la nueva consola Enterprise que se cree. Para consultar un ejemplo sobre cómo utilizar el Personalizador de la consola en un caso práctico, consulte *Apéndice D*.

Siga estos pasos para crear consolas con funciones limitadas:

1. Seleccione *Herramientas>Personalizador de la consola*.
2. Se mostrará el Personalizador de la consola.



3. Seleccione las funciones que se mostrarán en la nueva consola.
4. Haga clic en *Guardar como* para guardar la consola. Especifique un nombre para el archivo.
5. Cuando haga doble clic en el archivo *.exe* que se acaba de crear, se iniciará la consola con funcionalidad limitada.



Apagado de la consola Deep Freeze Enterprise

Para apagar la consola Deep Freeze, seleccione *Archivo* > *Salir* o haga clic en el botón para cerrar la ventana. Al salir, podrá elegir:

- Minimizar la consola en la bandeja del sistema.

  Esto no detiene la consola y mantiene las conexiones activas. El icono de la consola Deep Freeze aparece en la bandeja del sistema. Las tareas programadas seguirán ejecutándose. Para volver a abrir la consola Deep Freeze Enterprise, haga clic con el botón secundario en el icono de la barra de tareas y seleccione *Restaurar consola DF6*.

- Cerrar la consola Deep Freeze y dejar las conexiones de red en ejecución

  Esto cierra la consola, pero mantiene activas las conexiones con los equipos. Las tareas programadas seguirán ejecutándose.

- Cerrar la consola Deep Freeze y apagar las conexiones de red.

  Esto detiene los procesos de la consola, cierra las conexiones (incluido el servicio local) y no inicia la ejecución de las tareas programadas. Sin embargo, las tareas programadas que empezaron ejecutarse, seguirán con su ejecución.



Si se activa la opción *Establecer como predeterminado*, no se mostrará el cuadro de diálogo la próxima vez que salga de Deep Freeze. Para editar estos ajustes seleccione *Herramientas >Opciones de salida*.



Instalación de Deep Freeze en las estaciones de trabajo

Una vez creado un archivo de programa de instalación personalizado por medio del Administrador de configuración, Deep Freeze puede implementarse en los equipos mediante una instalación con supervisión, una instalación localizada, el sistema de instalación silenciosa o como parte de un proceso de imágenes.

Antes de realizar la instalación, se deben deshabilitar todas las utilidades y programas que se estén ejecutando en segundo plano, y cerrar todas las aplicaciones abiertas. Estos programas pueden interferir con la instalación y Deep Freeze podría no funcionar correctamente.

El equipo se reiniciará después de que se haya completado cualquier tipo de instalación. Deep Freeze debe estar en modo Descongelado para que se complete con éxito cualquier tipo de desinstalación.

Durante la instalación, se eliminarán todos los ThawSpace existentes si:

- no se ha activado la opción relativa a conservar los ThawSpace existentes en el Administrador de configuración
- el ThawSpace no se ha creado con Deep Freeze Enterprise v5 o posterior.

Instalación o desinstalación con supervisión

Para instalar o desinstalar Deep Freeze, siga estos pasos:

1. Ejecute el archivo de programa de instalación (*DFWks.exe*) en el equipo. Aparecerá la siguiente pantalla:
2. Haga clic en *Instalar* para iniciar la instalación. Siga los pasos que se muestran en la pantalla y acepte el contrato de licencia. Se instalará Deep Freeze y se reiniciará el equipo.



Para desinstalar Deep Freeze, haga clic en la opción *Desinstalar*. Solo se puede hacer clic en Desinstalar si previamente se ha instalado Deep Freeze en el equipo y si este está en modo Descongelado. Si hay un ThawSpace existente, Deep Freeze mostrará un cuadro de diálogo para que seleccione si desea conservarlo o eliminarlo.



Si la unidad de disco duro está demasiado fragmentada, no es posible crear ThawSpaces Se mostrará un mensaje que le pedirá que cancele la instalación o que instale Deep Freeze sin un ThawSpace.



Si selecciona *Posponer reinicio como congelado para completar las actualizaciones de Windows* (ficha Opciones avanzadas en el Administrador de configuración) e instala Deep Freeze, el instalador comprobará si se han completado todas las actualizaciones de Windows. Si no se han completado, no se llevará a cabo la instalación de Deep Freeze. Complete las actualizaciones de Windows y pruebe a instalar Deep Freeze de nuevo.

Si desactiva *Posponer reinicio como congelado para completar las actualizaciones de Windows* e instala Deep Freeze, compruebe que se hayan completado todas las actualizaciones de Windows sin utilizar Deep Freeze. Si desactiva esta opción, el equipo puede quedar atrapado en un ciclo de reinicios debido a las actualizaciones de Windows incompletas.



Desinstalación de Deep Freeze en la estación de trabajo a través de la consola

La consola Enterprise puede utilizarse para desinstalar Deep Freeze por completo o para desinstalar Deep Freeze pero dejando la semilla de estación de trabajo. Para poder desinstalar el programa, el equipo debe estar en modo Descongelado.

Para desinstalar Deep Freeze de un equipo y dejar la semilla de estación de trabajo, haga clic con el botón secundario en las estaciones de trabajo en modo Descongelado y seleccione *Desinstalar (Dejar semilla)*, como se muestra arriba. O haga clic en el icono de la barra de herramientas.

Para desinstalar por completo Deep Freeze y la semilla de estación de trabajo, seleccione los equipos que desea desinstalar y haga clic en el icono *Desinstalar* de la barra de herramientas.



Para poder desinstalar Deep Freeze, el equipo debe estar en modo Descongelado. La consola Enterprise solicitará una confirmación. Una vez confirmada la desinstalación, se desinstalará Deep Freeze y se reiniciará el equipo.



Instalación o desinstalación silenciosa

El Sistema de instalación silenciosa permite instalar Deep Freeze rápidamente en varias equipos de una red. Todas las utilidades de implementación que permiten la ejecución de una línea de comandos en un equipo remota pueden implementar el Sistema de instalación silenciosa. Una vez completada la instalación silenciosa, el equipo se reinicia automáticamente. La línea de comandos incluye las opciones siguientes:

Sintaxis	Descripción
`[/Install]`	Instala Deep Freeze mediante el archivo de instalación
`[/Install /Seed]`	Instala solamente el archivo de semilla de estación de trabajo especificado
`[/Install /Thawed]`	Instala Deep Freeze con el archivo de instalación y reinicia el equipo en modo Descongelado.
`[/Uninstall]`	Desinstala Deep Freeze
`[/Uninstall /Seed]`	Desinstala Deep Freeze y deja instalada la semilla de estación de trabajo
`[/PW=contraseña]`	Establece una contraseña durante la instalación*
`[/AllowTimeChange]`	Permite cambiar el reloj del sistema*
`[/Freeze=C,D,...]`	Pone en modo Congelado las unidades especificadas (y en modo Descongelado las demás)*
`[/Thaw=C,D,...]`	Poner en modo Descongelado las unidades especificadas (y en modo Congelado las demás)*
`[/USB]`	No protege los discos duros USB externos
`[/FireWire]`	No protege los discos duros FireWire externos

Ejemplo de línea de comandos

```
DFWks.exe /Install /Freeze=C /PW=contraseña
```

En el ejemplo que se muestra arriba, el archivo de programa de instalación de Deep Freeze se llama *DFWks.exe*. Solamente se pondrá la unidad C: en modo Congelado. Todas las demás unidades del equipo estarán en modo Descongelado. Si el equipo solo tiene una unidad C:, puede omitirse el parámetro [/Freeze]. Se creará una contraseña (contraseña). Después de ejecutarse el comando, se instalará Deep Freeze y se reiniciará el equipo en modo Congelado, listo para utilizarse.

El Sistema de instalación silenciosa no funciona sin el parámetro `[/Install]` o `[/Uninstall]`. Deep Freeze debe estar en modo Descongelado para de poder utilizar `[/Uninstall]`.



Para ejecutar las opciones de configuración de la línea de comandos, es preciso desactivar Deshabilitar opciones de línea de comandos en la ficha Opciones avanzadas.





* Estas opciones están deshabilitadas de forma predeterminada.

Instalación o desinstalación silenciosa a través de un acceso directo

Es posible instalar Deep Freeze directamente en un equipo sin tener que usar el cuadro de diálogo de instalación. Siga estos pasos.

1. Localice el archivo del programa de instalación de Deep Freeze (*DFWks.exe*) en el equipo de destino.
2. Haga clic con el botón secundario en el icono y seleccione *Crear acceso directo*.
3. Haga clic con el botón secundario en el acceso directo y seleccione *Propiedades*.
4. Para editar la ruta del campo Destino escriba `/install` o `/uninstall` al final de la ruta.

Ejemplo de destino de acceso directo:
`C:\Documents and Settings\DFWks.exe /install`

Al hacer doble clic en el nuevo acceso directo, Deep Freeze se instalará o desinstalará de inmediato, y se reiniciará el equipo.

Deep Freeze debe estar en modo Descongelado para poder utilizar `/uninstall`.



Si la unidad de disco duro está demasiado fragmentada, no es posible crear ThawSpaces y se cancelará la instalación.



Si selecciona *Posponer reinicio como congelado para completar las actualizaciones de Windows* (ficha Opciones avanzadas en el Administrador de configuración) e instala Deep Freeze, el instalador comprobará si se han completado todas las actualizaciones de Windows. Si no se han completado, no se llevará a cabo la instalación de Deep Freeze. Complete las actualizaciones de Windows y pruebe a instalar Deep Freeze de nuevo.

Si desactiva *Posponer reinicio como congelado para completar las actualizaciones de Windows* e instala Deep Freeze, compruebe que se hayan completado todas las actualizaciones de Windows sin utilizar Deep Freeze. Si desactiva esta opción, el equipo puede quedar atrapado en un ciclo de reinicios debido a las actualizaciones de Windows incompletas.

Instalación de red en varios equipos

El Sistema de instalación silenciosa también se puede utilizar para instalar Deep Freeze en varias equipos de una red. Si las estaciones de trabajo de la red utilizan secuencias de comandos para iniciar sesión, las secuencias de comandos pueden usarse para instalar Deep Freeze automáticamente en todas las estaciones de trabajo de la red. Todas las estaciones de trabajo se iniciarán en modo Congelado, listas para ser utilizadas una vez que la instalación se haya completado.



Utilice una de las siguientes sintaxis de líneas de comandos para crear un archivo de registro de informe de error de instalación:

```
\\Server Name\Share Name\DFWks.exe /Install >> my.log
```

Instalación en versiones existentes de Deep Freeze

A menos que se utilice la función Actualizar software Deep Freeze (para Deep Freeze 6.5 y versiones posteriores), todas las versiones existentes de Deep Freeze deberán desinstalarse antes de realizar una nueva instalación de Deep Freeze.

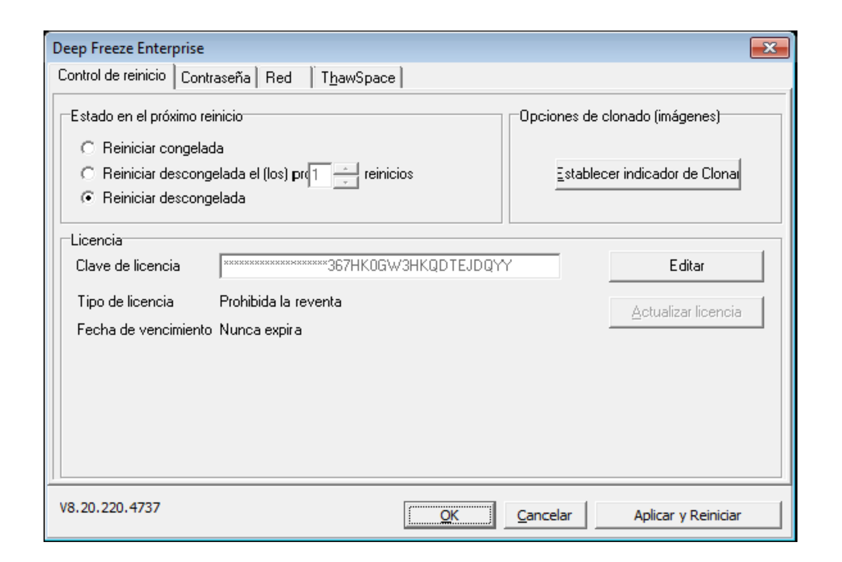
Instalación mediante imágenes

Deep Freeze ha sido diseñado para funcionar con los principales productos de software de gestión de escritorios y creación de imágenes. Use la instalación con supervisión o bien la instalación silenciosa para instalar Deep Freeze en una imagen maestra.

Es preciso preparar Deep Freeze para la implementación antes de finalizar la imagen maestra. Para preparar la imagen maestra para implementarla, siga estos pasos:

1. Reinicie el equipo en modo *Descongelado*.
2. Inicie Deep Freeze utilizando el método abreviado de teclado *CTRL+MAYÚS+ALT+F6*. También puede pulsar *Mayús* y hacer doble clic en el icono de Deep Freeze en la bandeja del sistema.
3. Introduzca la contraseña y haga clic en *Aceptar*.
4. Haga clic en *Establecer indicador de clonación* en la ficha *Control de reinicio*.
5. Aparecerá el mensaje *Se estableció el indicador con éxito*. *¿Desea reiniciar el equipo ahora?* Haga clic en *Sí* para reiniciar el equipo de inmediato. Haga clic en *No* para reiniciar el equipo más tarde.







El comando Establecer indicador de clonación es importante durante la creación de la imagen porque arranca el equipo en modo Descongelado si Deep Freeze no puede leer el archivo de configuración una vez se ha instalado la imagen correctamente.

Si no se establece el indicador de clonación y Deep Freeze no puede leer el archivo de configuración, se congelarán todas las unidades una vez se haya instalado la imagen correctamente.



Si va a utilizar Sysprep, asegúrese de establecer el indicador de clonación después de preparar el sistema para la creación de la imagen antes de iniciar Sysprep.

Después de crear la imagen, los equipos deben reiniciarse una vez más para que Deep Freeze pueda detectar correctamente los cambios en la configuración del disco. Si la imagen se instala en los equipos en modo no supervisado, deberá tomar medidas para asegurarse de que los equipos se reinicien y así permitan que se actualice la configuración.

Para volver al modo Congelado después de la creación de la imagen, configure Deep Freeze para que se reinicie en modo Descongelado los próximos *n* reinicios (en la imagen maestra). De esa manera, después de *n* reinicios, el equipo entrará en modo Congelado de forma automática. También puede utilizar el control de la línea de comandos de Deep Freeze para poner los equipos seleccionadas en modo Congelado.

Instalación localizada

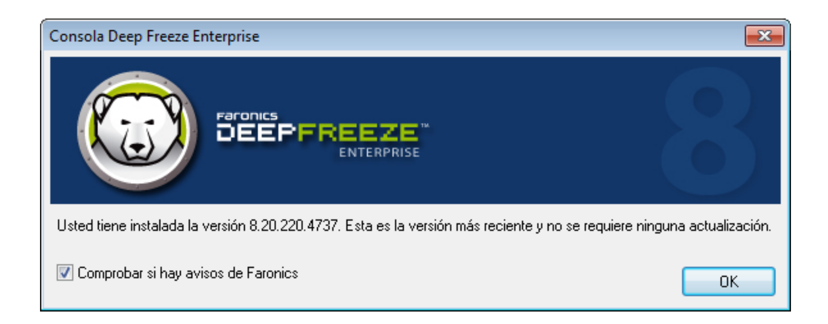
También es posible implementar Deep Freeze por medio de una Instalación localizada desde la consola Enterprise.



Búsqueda de actualizaciones

Deep Freeze permite comprobar si hay nuevas versiones disponibles.

Vaya a *Ayuda* > *Buscar actualizaciones*. Se comprobará si hay nuevas versiones de Deep Freeze disponibles.



Si hay una nueva versión disponible, haga clic en *Descargar la última versión* para actualizar Deep Freeze.





Gestión de equipos con Deep Freeze

En este capítulo se describe la gestión de equipos en los que Deep Freeze está instalado.

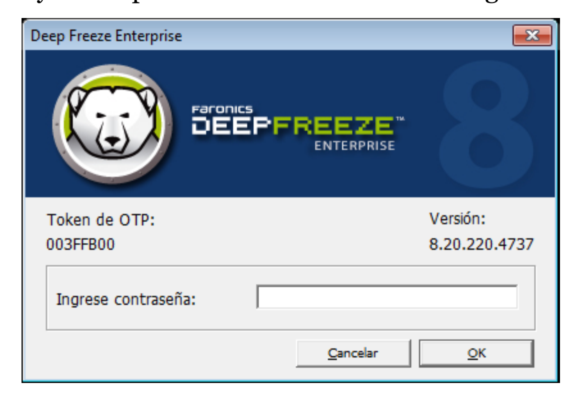
Temas



Pantalla de inicio de sesión

Utilice uno de los siguientes métodos para acceder a Deep Freeze desde un equipo.

1. Si el icono de Deep Freeze aparece en la bandeja del sistema, mantenga pulsada la tecla Mayús y haga doble clic en el icono de Deep Freeze. Si Deep Freeze se ejecuta en Modo invisible y el icono de Deep Freeze no aparece, deberá utilizarse el método abreviado de teclado CTRL+ALT+Mayús+F6 para accede al cuadro de diálogo de inicio de sesión.



2. Introduzca la contraseña del administrador y haga clic en *Aceptar* para iniciar sesión en Deep Freeze.

Como función de seguridad adicional, Deep Freeze evita "ataques de fuerza bruta" al reiniciar automáticamente el equipo después de 10 intentos de conexión fallidos.

Iniciar Deep Freeze en dispositivos con pantalla táctil

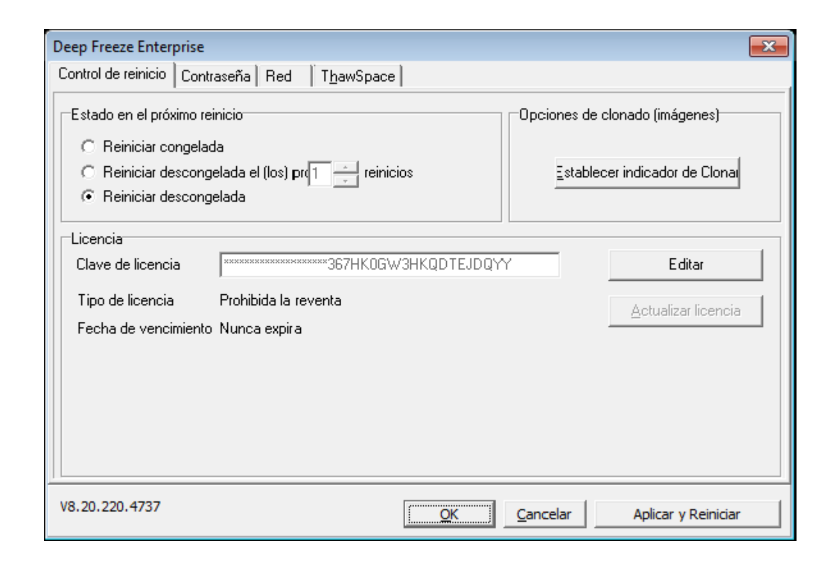
Puede utilizar Ctrl+Alt+Mayús+6 o Ctrl+Alt+Mayús+F6 para iniciar Deep Freeze en dispositivos con pantalla táctil. Sin embargo, debe habilitar el teclado completo antes de utilizar este método abreviado. También puede mantener pulsada la bandeja del sistema para abrir el menú contextual de Deep Freeze.

Ficha Estado

La ficha *Estado* muestra las siguientes opciones:

Estado en el próximo reinicio

La ficha Estado permite configurar el estado de Deep Freeze después del próximo reinicio.



Seleccione una de las siguientes opciones:

- *Reiniciar como Congelado*

  para asegurarse de que el equipo aparezca en modo Congelado la próxima vez que se reinicie.
- *Reiniciar como Descongelado la próxima vez*

  para asegurarse de que el equipo aparezca en modo Descongelado cada vez que se reinicie durante un número de reinicios especificado. Cuando se exceda dicho número de reinicios, el equipo se reiniciará en modo Congelado.
- *Reiniciar como Congelado*

  para garantizar que el equipo aparezca en modo Congelado cada vez que se reinicie

Seleccione el botón de opción junto a la opción deseada y haga clic en *Aceptar* para guardar los cambios. Al hacer clic en *Aplicar* y *Reiniciar*, se guardarán todos los cambios y se reiniciará el equipo inmediatamente.

Clonar

El panel *Clonar* se usa para preparar las imágenes maestras para el proceso de implementación. Para obtener más información, consulte la sección *Instalación mediante imágenes*.



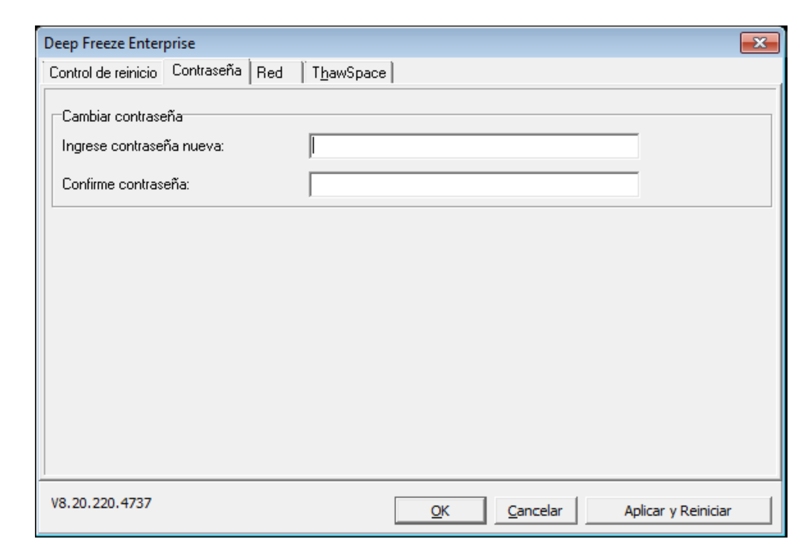
Licencia

Introduzca la clave de licencia en el campo *Clave de licencia*. Si no se introduce una clave de licencia, Deep Freeze caducará a los 30 días de la instalación.



Ficha Contraseña

La ficha *Contraseña* permite cambiar la contraseña.

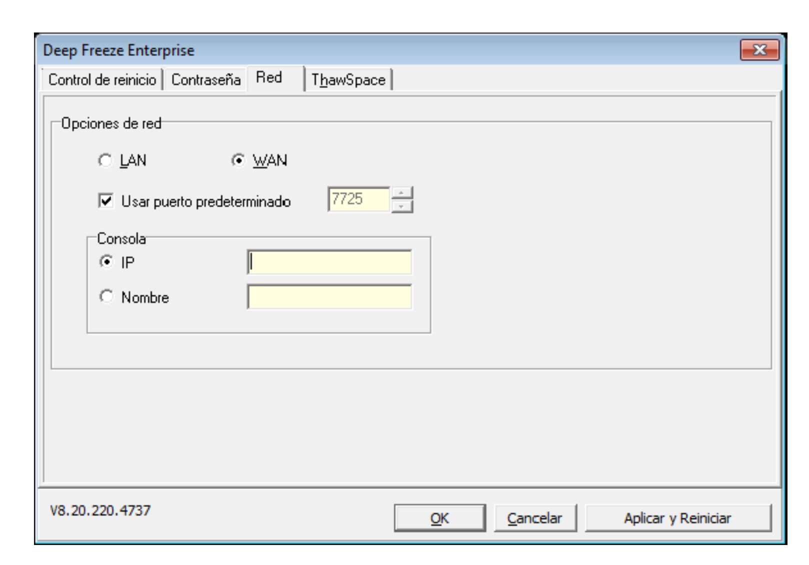


1. Especifique una nueva contraseña en el campo *Introducir nueva contraseña*.
2. Confirme la nueva contraseña introduciendo la misma contraseña en el campo *Confirmar contraseña* .
3. Haga clic en Aceptar.
4. Se cambiará la contraseña y se mostrará un cuadro de diálogo de confirmación.



Ficha Red

La ficha *Red* permite configurar las opciones de red en un equipo.



Para elegir el método de comunicación *LAN* o *WAN* haga clic en la opción deseada.

Si desea cambiar el número de puerto predeterminado, desactive la casilla de verificación *Usar puerto predeterminado* e introduzca el número de puerto deseado.

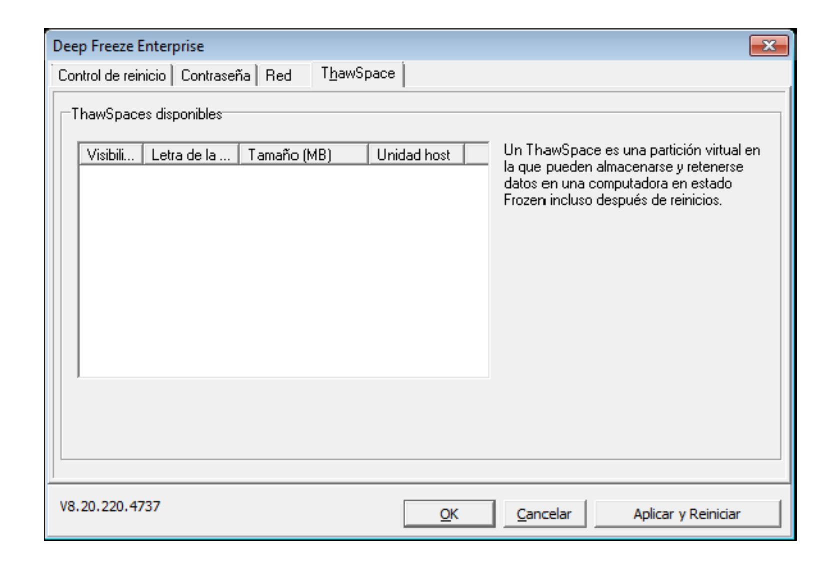
Para obtener más información sobre la configuración de red, consulte *Apéndice B*.



Ficha ThawSpace

ThawSpace es una partición virtual en un equipo que puede utilizarse para almacenar programas, guardar archivos o realizar cambios permanentes. Todos los archivos almacenados en el ThawSpace se conservarán después de un reinicio, aunque el equipo esté en modo Congelado.

Para que el ThawSpace esté disponible, es preciso configurar su creación en el Administrador de configuración de Deep Freeze.



Después de desinstalar Deep Freeze, todos los ThawSpaces serán visibles. Si se vuelve a instalar Deep Freeze, los ThawSpaces estarán en modo *Visible* u *Oculto* en función de la configuración original especificada en la ficha ThawSpace.

Los ThawSpaces existentes se eliminarán durante una desinstalación, si se aplica alguno de estos casos:

- no se ha seleccionado la opción relativa a conservar los ThawSpace existentes en el *Administrador de configuración*
- el ThawSpace no se ha creado con Deep Freeze Enterprise 5 o posterior.



Instalaciones, modificaciones o eliminaciones de software permanentes

Para que los cambios surtan efecto, es necesario poner los equipos en modo Descongelado. Para instalar un software, a menudo es necesario reiniciar el equipo una o dos veces para completar la instalación.

Deep Freeze ayuda a los administradores a superar las dificultades que implica mantener la configuración de sus equipos en un ambiente de producción. Deep Freeze protege los equipos de cambios no autorizados, virus y programas maliciosos que pueden el equipo en estado no funcional. Deep Freeze también incluye funciones para conservar los datos de usuario mientras protege el equipo.

Para obtener más información sobre cómo implementar Deep Freeze y garantizar la conservación de la información de usuario, consulte *Deep Freeze - Retaining User Data (Deep Freeze: conservación de la información de usuario)* disponible en *http://www.faronics.com/library*



Administración de Anti-Virus

En este capítulo se describe la instalación y el uso de Anti-Virus con la consola Enterprise.

Temas



Información general sobre Anti-Virus

Anti-Virus se puede instalar y usar a través de la consola Enterprise. El uso de Anti-Virus es opcional. También se puede usar Deep Freeze Enterprise sin usar Anti-Virus.

Se explican las siguientes secciones:

- Habilitar Anti-Virus en la consola Enterprise
- Instalar el cliente de Anti-Virus en la estación de trabajo
- Configuración de Anti-Virus
- Usar Anti-Virus desde la consola Enterprise
- Programar tareas de Anti-Virus
- Usar el cliente de Anti-Virus en la estación de trabajo
- Buscar actualizaciones
- Actualizar Faronics Anti-Virus
- Desinstalar el cliente de Anti-Virus en la estación de trabajo
- Deshabilitar Anti-Virus en la consola Enterprise



Habilitar Anti-Virus en la consola Enterprise

Ahora, Anti-Virus forma parte de la consola Enterprise y se puede habilitar desde la misma. Es preciso comprar una licencia aparte para Anti-Virus.

Siga los pasos descritos a continuación para habilitar Faronics Anti-Virus:

1. Inicie la consola Deep Freeze Enterprise.
2. Vaya a *Herramientas* > *Licencias* > *Licencia de Faronics Anti-Virus*.
3. Active la casilla de verificación *Deseo usar la consola Deep Freeze para administrar Faronics Anti-Virus*.
4. Haga clic en *Editar*.
5. Introduzca la clave de licencia y haga clic en *Actualizar licencia*.
6. Haga clic en *Cerrar*. Se descargarán los archivos del instalador de Anti-Virus. Se mostrarán las columnas de Anti-Virus en el panel Estación de trabajo. Se agregará el subnodo Anti-Virus en *Configuración disponible* en el panel Red y grupos.



Instalar el cliente de Anti-Virus en la estación de trabajo

Antes de instalar Anti-Virus en la estación de trabajo, asegúrese de que se haya implementado el archivo de instalación de estación de trabajo de Deep Freeze o la semilla de Deep Freeze, y que la estación de trabajo esté en modo Descongelado.

Siga los pasos descritos a continuación para instalar Anti-Virus en la estación de trabajo:

1. Seleccione una estación de trabajo (o varias estaciones de trabajo) en el panel *Estaciones de trabajo > Anti-Virus*.
2. Haga clic en el icono de Anti-Virus en la barra de menús y seleccione *Instalar Faronics Anti-Virus*.
3. Active la casilla de verificación *Quitar cualquier producto antivirus no compatible antes de instalar Faronics Anti-Virus* para quitar los programas antivirus existentes.
4. Haga clic en *Aceptar* para confirmar la acción.

Se reiniciará la estación de trabajo y se instalará el cliente de Anti-Virus en las estaciones de trabajo.

Se habilitarán las opciones de Anti-Virus en la ficha Anti-Virus.



Configuración de Anti-Virus

Una configuración de Anti-Virus contiene todos los ajustes acerca de cómo se debe ejecutar Anti-Virus en las estaciones de trabajo. Incluye las acciones que debe realizar el programa, las programaciones, los servidores proxy, los informes de error y las funciones permitidas al usuario en la estación de trabajo. En las siguientes secciones se explica cómo crear y aplicar una configuración de Anti-Virus.



Anti-Virus contiene una configuración *Predeterminada*. La configuración Predeterminada contiene los ajustes de configuración más óptimos para administrar Anti-Virus.

Creación de una configuración de Anti-Virus

Realice los siguientes pasos para crear una nueva configuración de Anti-Virus:

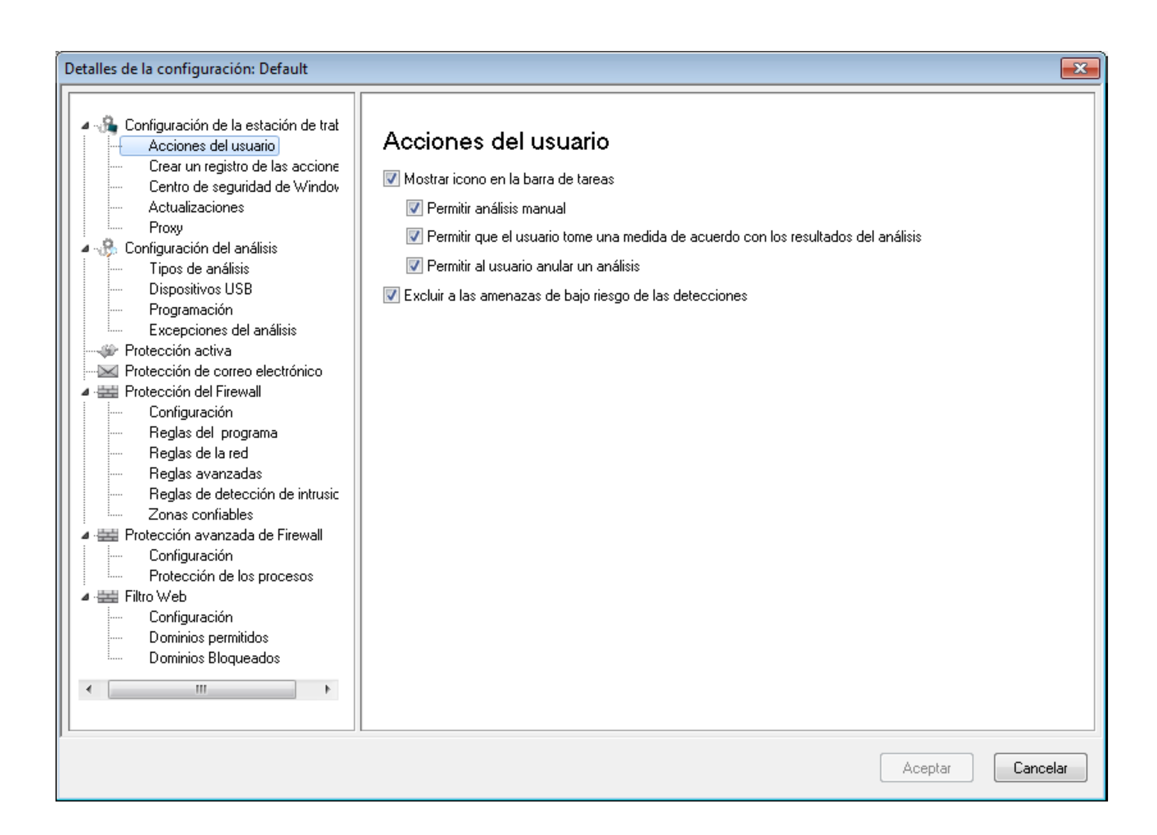
1. Inicie la consola Enterprise.
2. En el panel *Red y grupos*, vaya a *Configuraciones disponibles* > *AntiVirus*.
3. Haga clic con el botón secundario y seleccione *Crear nueva configuración*.



4. Especifique los ajustes en el nodo *Configuración de estación de trabajo*:



- Nodo *Configuración de estación de trabajo* > panel *Acciones de usuario*



— *Mostrar icono de barra de tareas*: active esta casilla de verificación para mostrar el icono de Faronics Anti-Virus en la barra de tareas de las estaciones de trabajo. Si no se activa esta casilla de verificación, Faronics Anti-Virus permanecerá oculto para el usuario.

— *Permitir análisis manual*: active esta casilla de verificación para permitir a los usuarios iniciar de forma manual el análisis de Faronics Anti-Virus en las estaciones de trabajo.

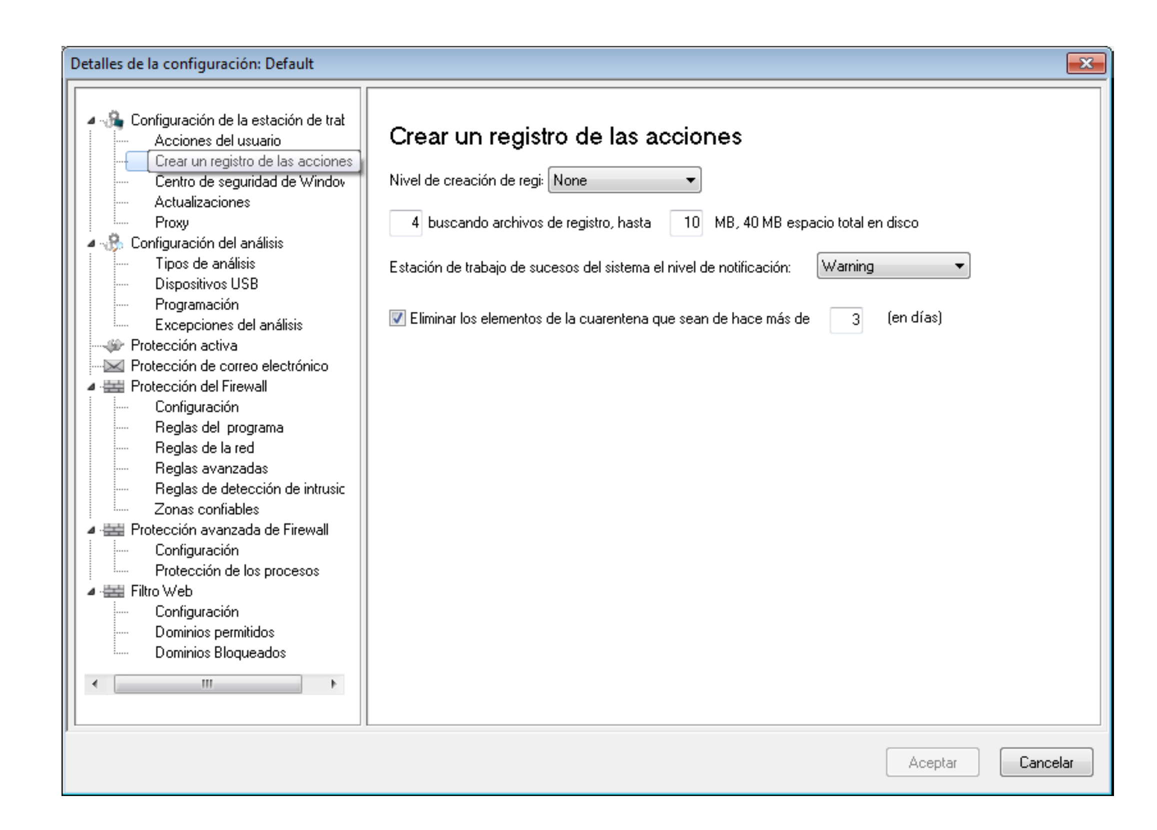
— *Permitir al usuario tomar medidas sobre los resultados del análisis*: active esta casilla de verificación para permitir al usuario de la estación de trabajo tomar medidas en función de los resultados del análisis.

— *Permitir al usuario anular un análisis iniciado localmente*: active esta casilla de verificación para permitir a los usuarios anular un análisis iniciado localmente en la estación de trabajo.

— *Excluir amenazas de bajo riesgo de detecciones*: seleccione esta casilla de verificación para excluir las amenazas de bajo riesgo de las detecciones. Las amenazas de bajo riesgo son aquellas que no repercuten de forma negativa en el sistema (por ejemplo, cookies).



- Nodo *Configuración de estación de trabajo>Acciones de registro*



— *Nivel de registro*: seleccione el nivel de registro. Seleccione *Ninguno* si no desea que se realice ningún tipo de registro. Seleccione *Error* para registrar los mensajes de error. Seleccione *Seguimiento* para realizar un seguimiento. Seleccione *Detallado* si desea que el registro incluya información detallada.

— *Número de archivos de registro*: especifique el número de archivos de registro. La información de registro se guardará de forma secuencial en los archivos. Por ejemplo, si hay tres archivos A, B y C, Faronics Anti-Virus escribirá primero los registros de error en el archivo A. Una vez que este esté lleno, los escribirá en el archivo B y, por último, en el archivo C. Cuando el archivo C esté lleno, se borrarán los datos en el archivo A y se escribirán los nuevos datos.

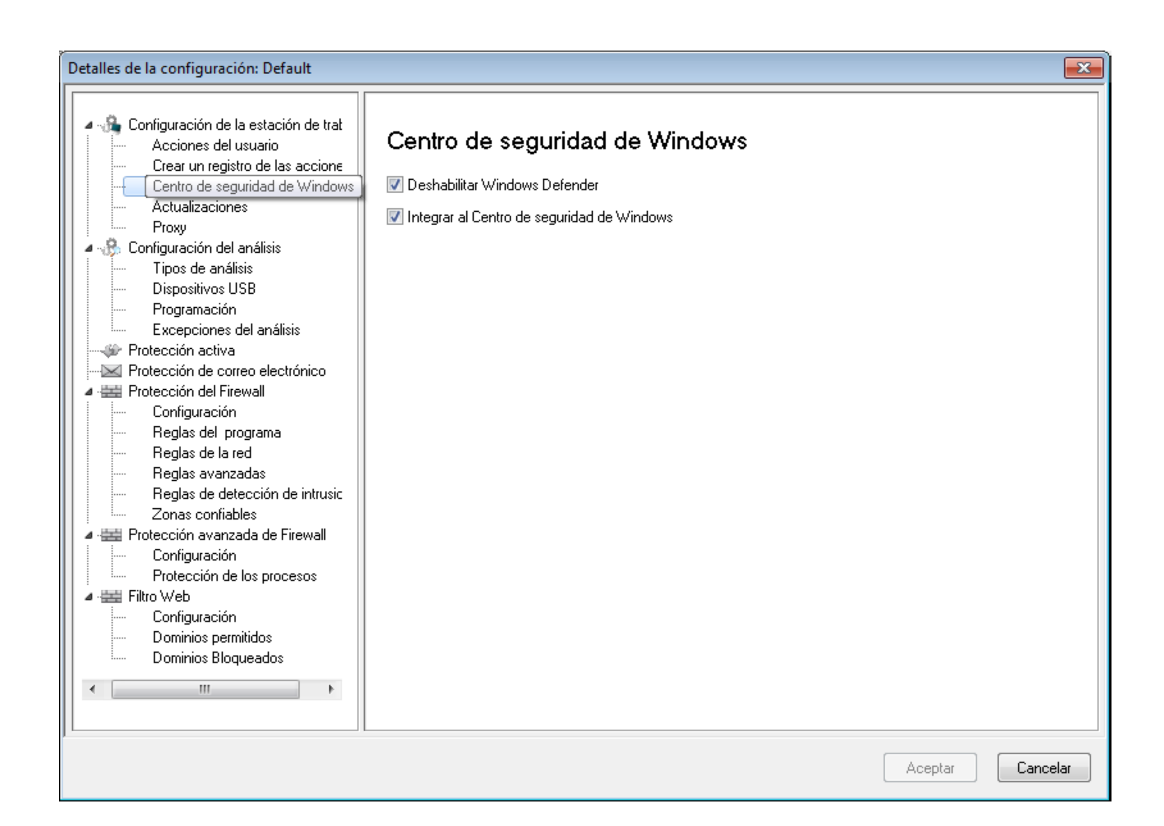
— *Tamaño de archivo*: seleccione el tamaño de cada uno de los archivos en MB.

— *Nivel de informe de eventos del sistema de estación de trabajo*: seleccione Ninguno, Error, Advertencia o Información.

— *Eliminar elementos en cuarentena que tengan más de*: especifique el número de días que se deberán conservar los elementos en cuarentena. El valor predeterminado es 3 días.



- Nodo *Configuración de estación de trabajo* > panel *Centro de seguridad de Windows*

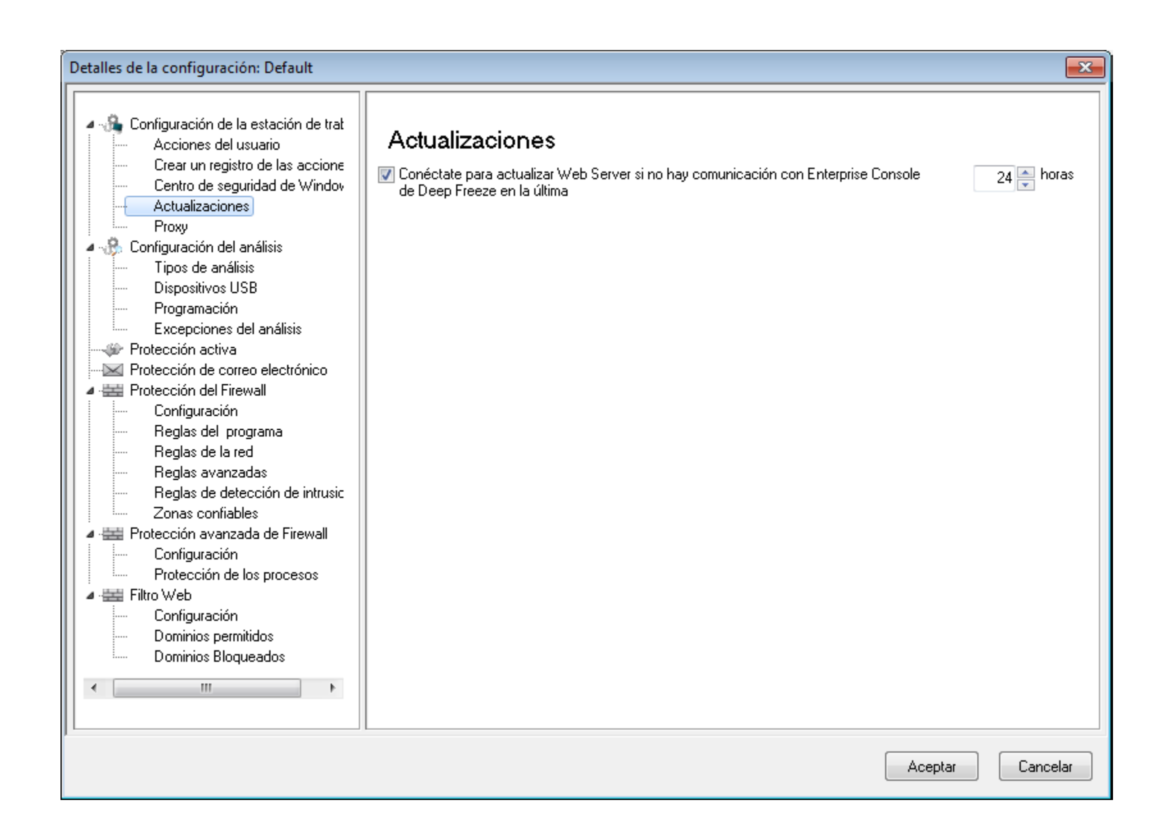


— *Deshabilitar Windows Defender*: active esta casilla de verificación para deshabilitar Windows Defender. Esto permite evitar un posible conflicto entre Faronics Anti-Virus y Windows Defender. La ejecución de varios programas antivirus o antispyware puede crear un conflicto, ya que un programa puede confundir a otro con un virus o spyware. Asimismo, la ejecución de varios programas antivirus o antispyware puede aumentar la carga de trabajo del procesador y el uso de memoria. Si aún así desea que Windows Defender se siga ejecutando, puede elegir no deshabilitarlo.

— *Integrar en Centro de seguridad de Windows*: active esta casilla de verificación para integrar Faronics Anti-Virus en el Centro de seguridad de Windows. El Centro de seguridad de Windows indicará si Faronics Anti-Virus está activo o inactivo en la bandeja del sistema.



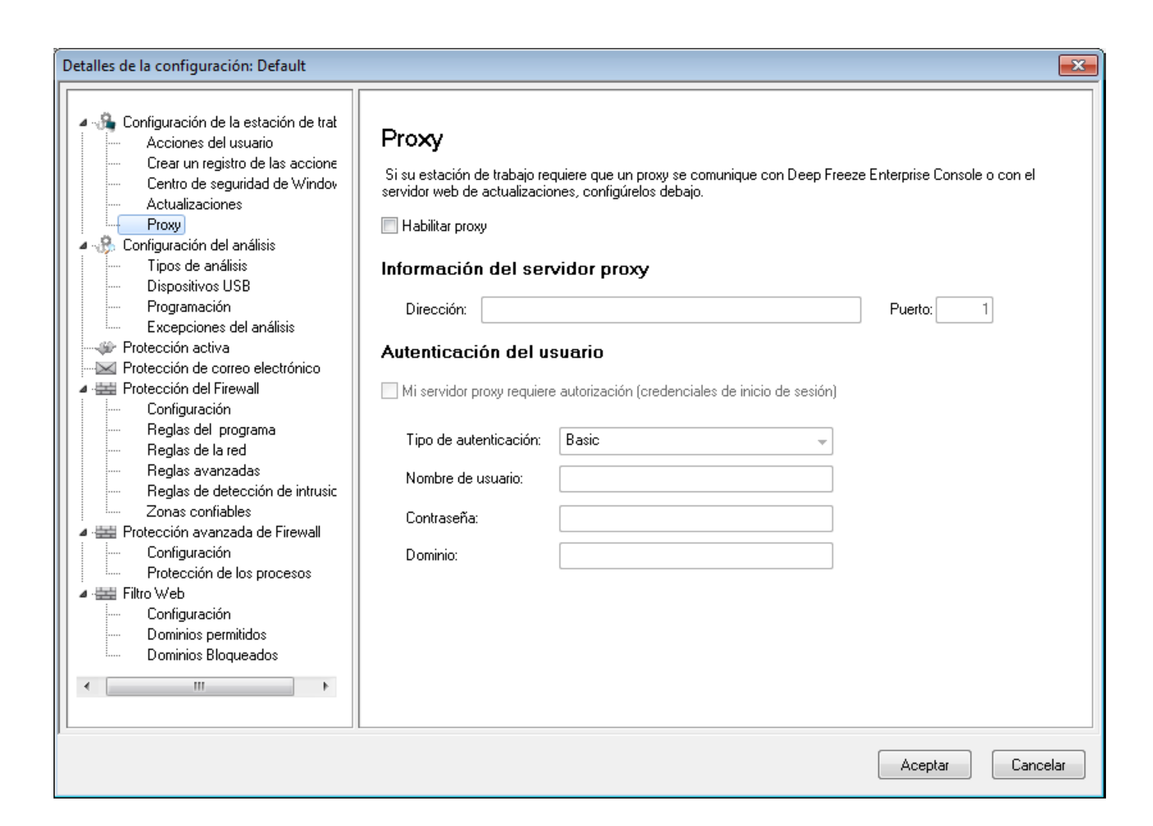
- *Nodo Configuración de estación de trabajo > panel* Actualizaciones



— *Comprobar si hay actualizaciones cada x horas*: seleccione la casilla de verificación para conectarse con el servidor web de actualizaciones y descargar las definiciones de virus.



- *Nodo Configuración de estación de trabajo > panel* Proxy

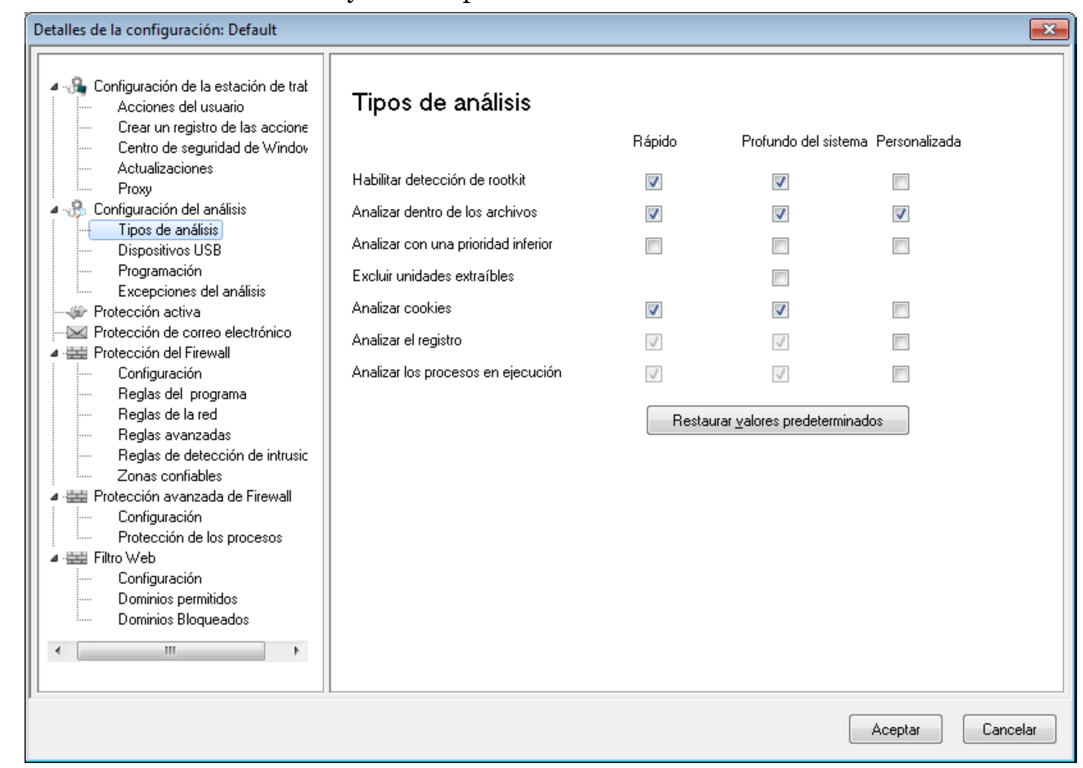


- *Habilitar proxy*: seleccione la casilla de verificación si las estaciones de trabajo necesitan un proxy para comunicarse con el servidor web de actualizaciones. Especifique la *Dirección* y el *Puerto*.
- *Mi servidor proxy requiere autorización (credenciales de inicio de sesión)*: si el servidor requiere autenticación, especifique los valores para los siguientes campos:
- *Tipo de autenticación*: seleccione el tipo de autenticación.
  - — *Nombre de usuario*: especifique el nombre de usuario.
  - — *Contraseña*: especifique la contraseña.
  - — *Dominio*: especifique el dominio.



5. Especifique los ajustes en el nodo *Análisis*:

- Nodo *Análisis* > panel *Configuración de análisis*: seleccione lo siguiente para análisis rápido, análisis a fondo del sistema y análisis personalizado:



Faronics Anti-Virus ofrece tres tipos de análisis:

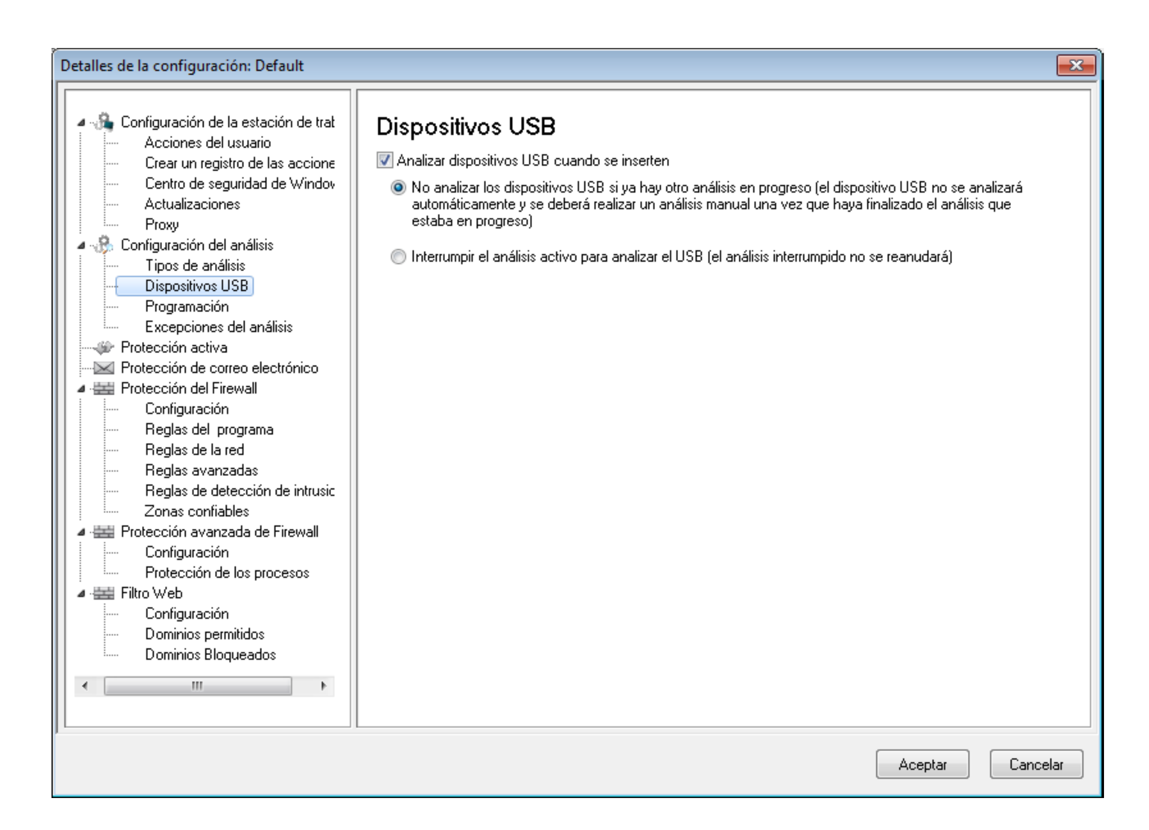
- *Análisis rápido*: analiza las áreas comúnmente afectadas de su equipo. Su duración es menor que el análisis a fondo del sistema. El análisis rápido también usa menos memoria que el análisis a fondo del sistema.
- *Análisis a fondo del sistema*: realiza un análisis minucioso de todas las áreas del equipo. La duración del análisis dependerá del tamaño de la unidad de disco duro.
- *Análisis personalizado*: realiza un análisis de acuerdo con las selecciones realizadas en cuadro de diálogo *Detalles de la configuración*.

Para cada tipo de análisis, seleccione las opciones siguientes (algunas opciones pueden aparecer atenuadas en función del tipo de análisis):

- *Habilitar detección de rootkits*: detecta si el equipo está infectado con un rootkit.
- *Analizar dentro de archivos*: analiza el contenido de los archivos zip. Seleccione esta opción si también desea que se analicen los archivos de almacenamiento, como .RAR y .ZIP. Si un archivo .RAR contiene un archivo infectado, el archivo .RAR se pondrá en cuarentena. Si un archivo .ZIP contiene un archivo infectado, el archivo infectado se pondrá en cuarentena y será reemplazado por un archivo .TXT con texto que informará al usuario de que el archivo estaba infectado y se ha puesto en cuarentena.
- *Analizar con prioridad baja*: seleccione esta opción si desea que Faronics Anti-Virus se ejecute con prioridad baja, de manera que los usuarios puedan seguir trabajando con otros programas sin que se vea afectado el rendimiento. Se recomienda seleccionar esta opción para análisis programados a horas en las que suelen utilizarse los equipos.
- *Excluir unidades extraíbles (p.ej., USB)*: excluye las unidades extraíbles del proceso de análisis. No se analizarán dispositivos como discos externos extraíbles, unidades USB, etc.



- *Analizar cookies*: analiza las cookies guardadas en la estación de trabajo.
- *Analizar el registro*: analiza el registro.
- *Analizar procesos en ejecución*: analiza los procesos que se están ejecutando en ese momento.
- *Nodo Análisis > panel Dispositivos USB*: especifique la siguiente configuración:



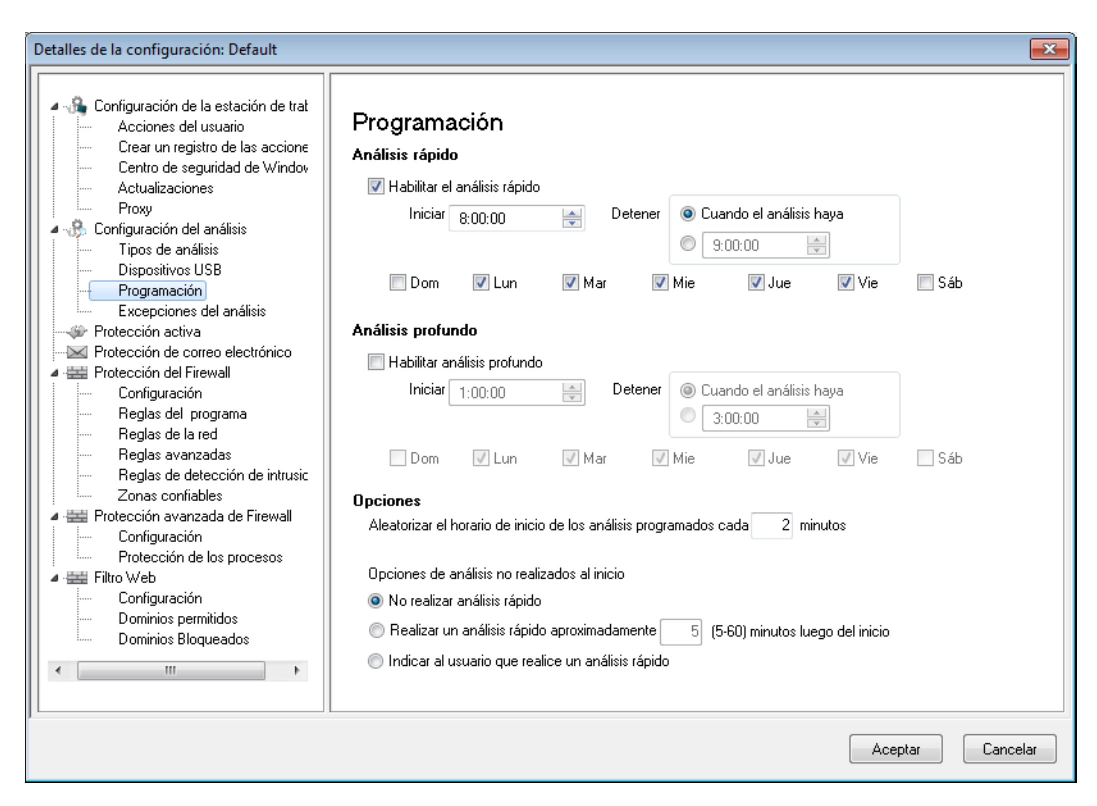
- *Analizar unidades USB al insertar*: active esta casilla de verificación para analizar las unidades USB cuando se conecten al equipo, y seleccione una de las opciones siguientes:
  — *No realizar análisis USB si ya hay otro análisis en curso*: seleccione esta opción para que el análisis activo no se interrumpa cuando se conecte una unidad USB. Una vez haya finalizado el análisis activo, se deberá iniciar el análisis de la unidad USB manualmente.
  — *Interrumpir análisis activo para analizar USB*: seleccione esta opción para interrumpir el análisis activo y analizar la unidad USB conectada. Una vez se haya interrumpido el análisis activo, este no se reanudará automáticamente, sino que deberá iniciarse manualmente.



Si la casilla de selección *Permitir análisis manual* está seleccionada en la ficha *Configuración de estación de trabajo* panel >*Acciones del usuario*, el dispositivo USB se analizará automáticamente. Si la casilla de verificación *Permitir análisis manual* no está seleccionada, el dispositivo USB no se analizará automáticamente.



- Nodo *Análisis* > panel *Programación*: especifique la siguiente configuración:



Análisis rápido:

- *Habilitar análisis rápido*: active esta casilla de verificación para habilitar el análisis rápido.
- *Inicio*: especifique la hora de inicio.
- *Finalización*: especifique la hora de finalización. El intervalo de tiempo máximo entre la hora de *Inicio* y la hora de *Finalización* es de *23.59* horas. Si se analizan todos los archivos antes de la hora de *Finalización*, finalizará el análisis. Si el análisis no se completa antes de la hora de *Finalización*, se interrumpirá cuando llegue a la hora de *Finalización*. También puede seleccionar *Cuando finalice el análisis* para asegurarse de que termine el análisis.
- *Días*: seleccione los días en los que se ejecutará el análisis rápido programado.

Análisis a fondo:

- *Habilitar análisis a fondo*: active esta casilla de verificación para habilitar el análisis a fondo.
- *Inicio*: especifique la hora de inicio.
- *Finalización*: especifique la hora de finalización. El intervalo de tiempo máximo entre la hora de *Inicio* y la hora de *Finalización* es de *23.59* horas. Si se analizan todos los archivos antes de la hora de *Finalización*, finalizará el análisis. Si el análisis no se completa antes de la hora de *Finalización*, se interrumpirá cuando llegue a la hora de *Finalización*. También puede seleccionar *Cuando finalice el análisis* para asegurarse de que termine el análisis.
- *Días*: seleccione los días en los que se ejecutará el análisis a fondo programado.



Opciones:

— *Horas de inicio de análisis programados aleatorias cada x minutos*: especifique el número de minutos. Los análisis programados se iniciarán de forma aleatoria para reducir el impacto en el tráfico de la red.

Opciones si no se realiza el análisis: seleccione una de las opciones siguientes para especificar cómo se debe realizar el análisis si la estación de trabajo no estaba *ENCENDIDA* durante un análisis programado:

— *No realizar análisis rápido*: seleccione esta opción si no desea realizar un análisis rápido al inicio.

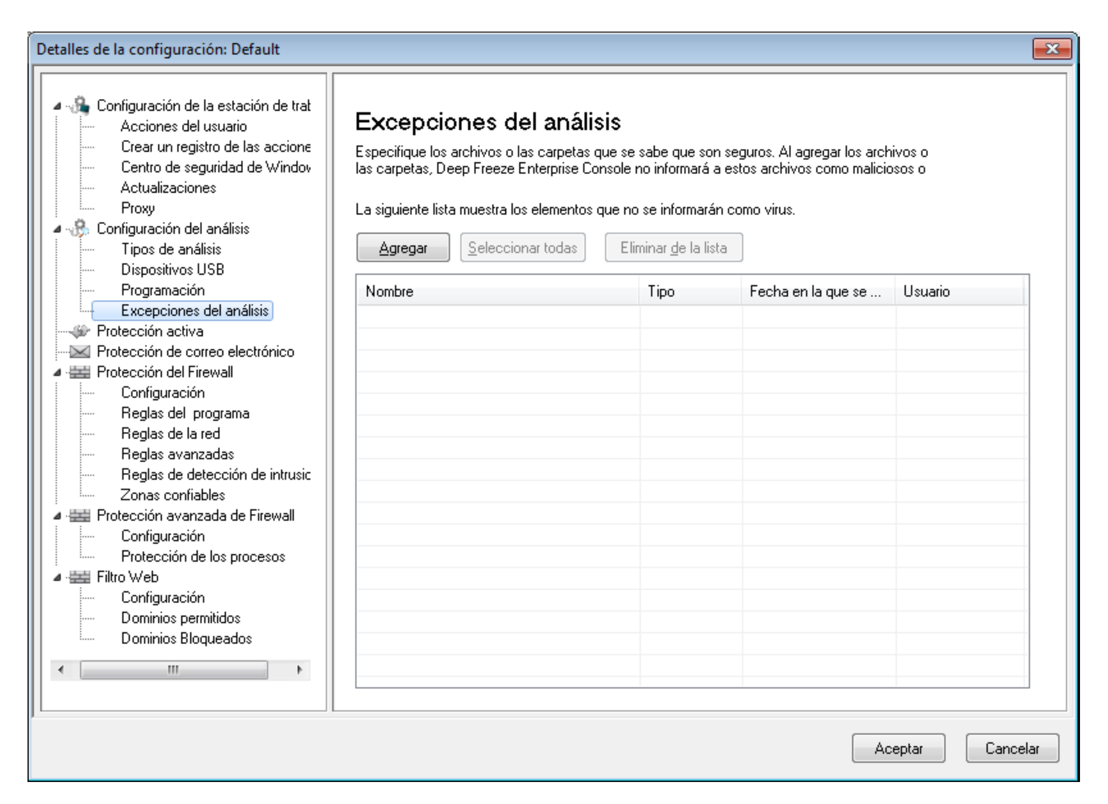
— *Realizar análisis rápido aproximadamente x minutos después del inicio*: especifique el número de minutos que deben transcurrir desde el inicio para que Faronics Anti-Virus inicie el análisis.

— *Preguntar al usuario si desea realizar un análisis rápido*: seleccione esta opción para preguntar al usuario si desea realizar un análisis rápido.

6. Especifique los ajustes en el nodo *Análisis* > panel *Excepciones de análisis*:

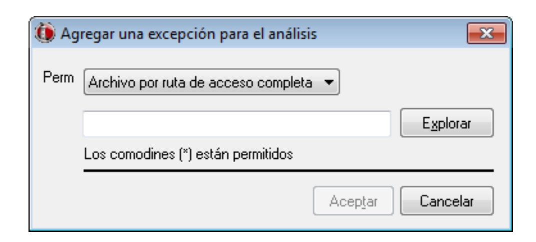
   La ficha Excepciones de análisis permite agregar carpetas o archivos identificados como seguros. Faronics Anti-Virus siempre analizará los archivos agregados a la ficha Excepciones de análisis. Sin embargo, nunca identificará los archivos como maliciosos o infectados. El administrador nunca recibirá notificaciones de amenazas de los archivos y carpetas especificados como seguros.

   a. Haga clic en *Agregar*.

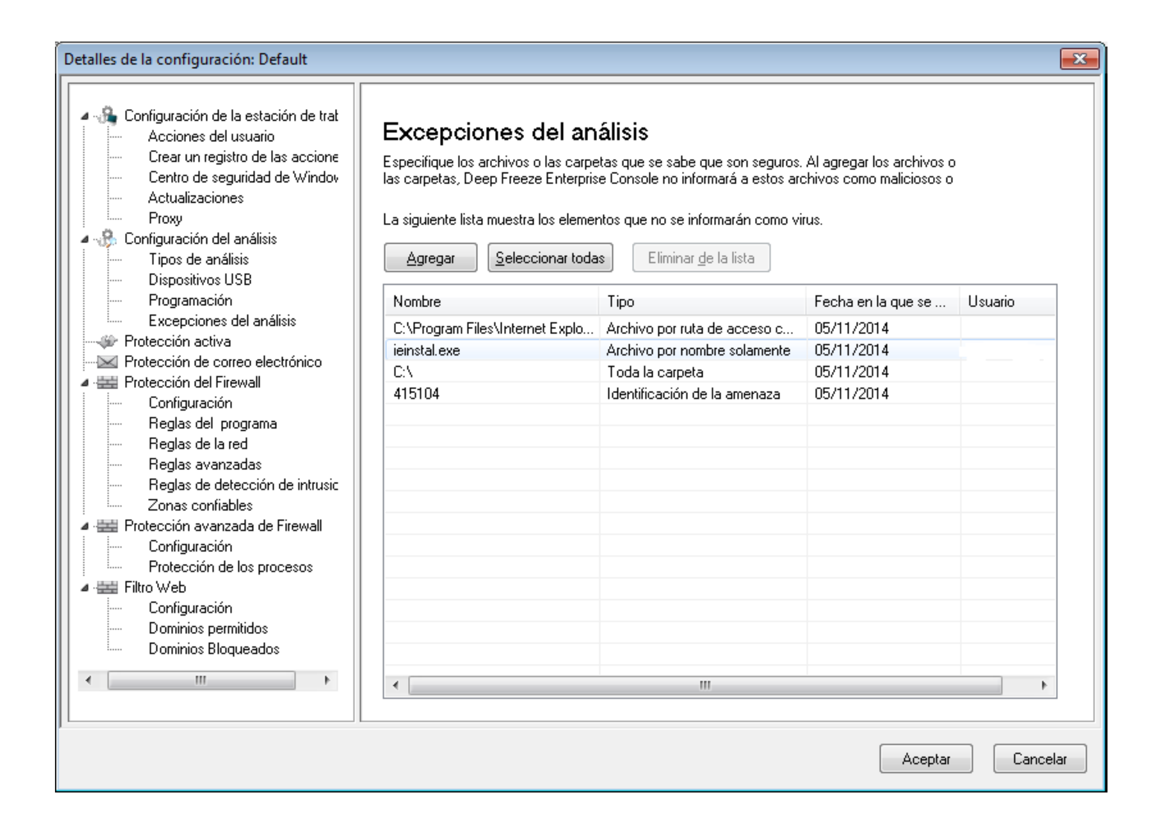


   b. En el cuadro de diálogo *Agregar*, seleccione *Archivo por ruta completa*, *Archivo solo por nombre*, *Toda la carpeta* o *Id. de amenaza*. Haga clic en Examinar para seleccionar el archivo o carpeta y haga clic en *Aceptar*.



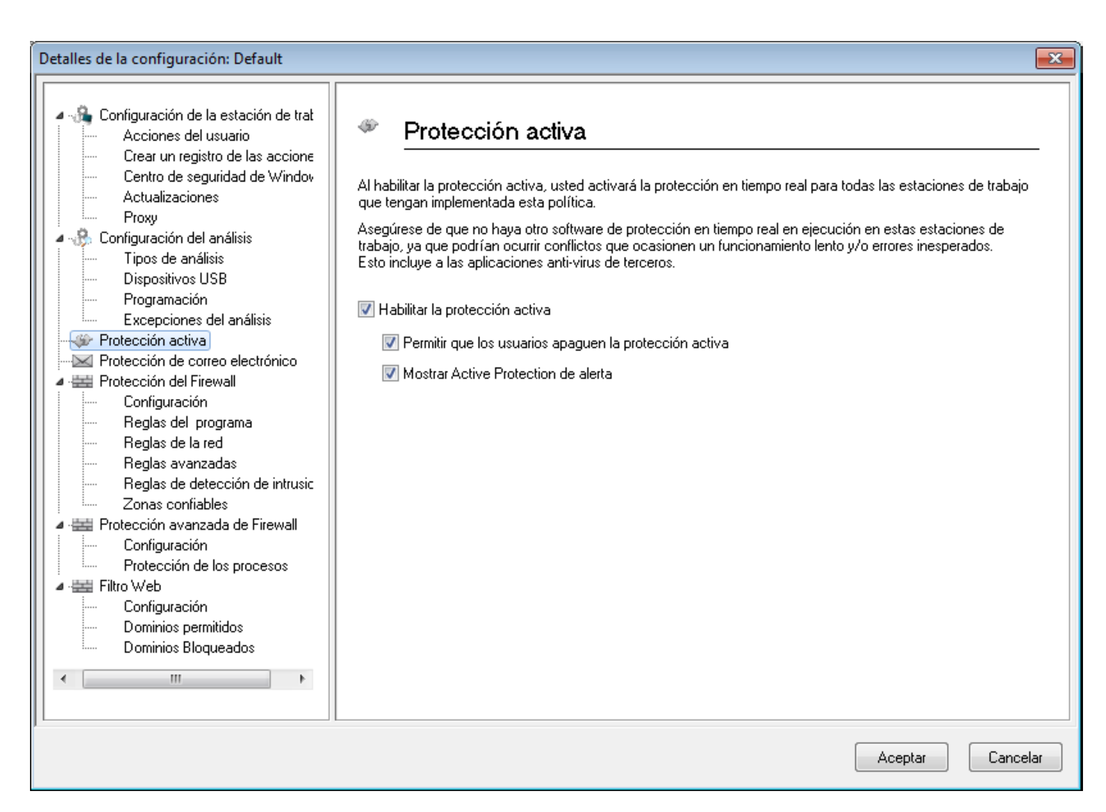


c. El *Archivo por ruta completa* se agregará a las excepciones de análisis.





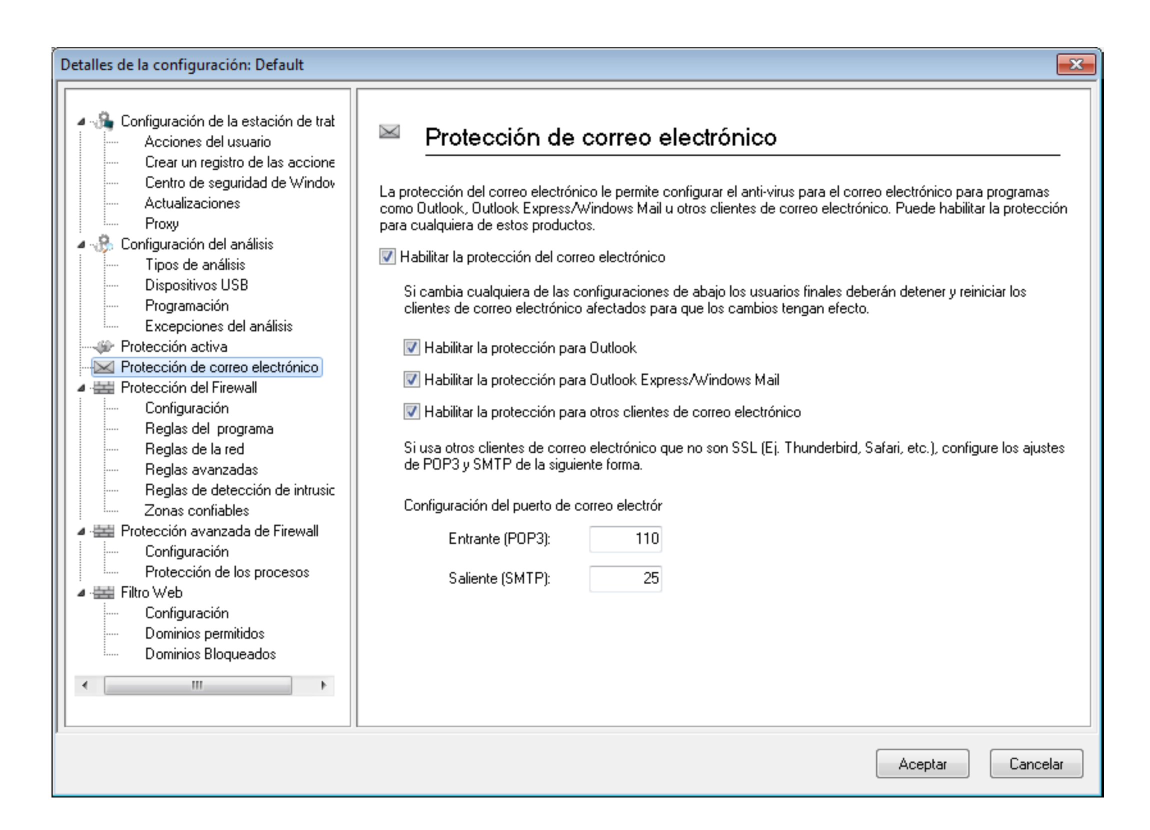
7. Especifique los ajustes en el panel *Protección activa*:



- *Habilitar protección activa*: seleccione esta opción para habilitar la protección en tiempo real. La protección activa es un análisis en tiempo real que se ejecuta en segundo plano sin comprometer el rendimiento del sistema. Seleccione esta opción si hay riesgo de infección de virus en tiempo real desde Internet.
- *Permitir al usuario desactivar la protección activa*: seleccione esta opción para permitir a los usuarios desactivar la protección activa. Seleccione esta opción si los usuarios instalan o utilizan software que podría ser identificado de forma errónea como virus (por ejemplo, la ejecución de macros avanzadas en Microsoft Office o archivos por lotes complejos).
- *Mostrar alerta de protección activa*: seleccione esta opción para mostrar una alerta si se detecta una amenaza durante la protección activa. No active esta casilla de verificación si no desea que se muestre una alerta.



8. Especifique los ajustes en el panel *Protección de correo electrónico*:



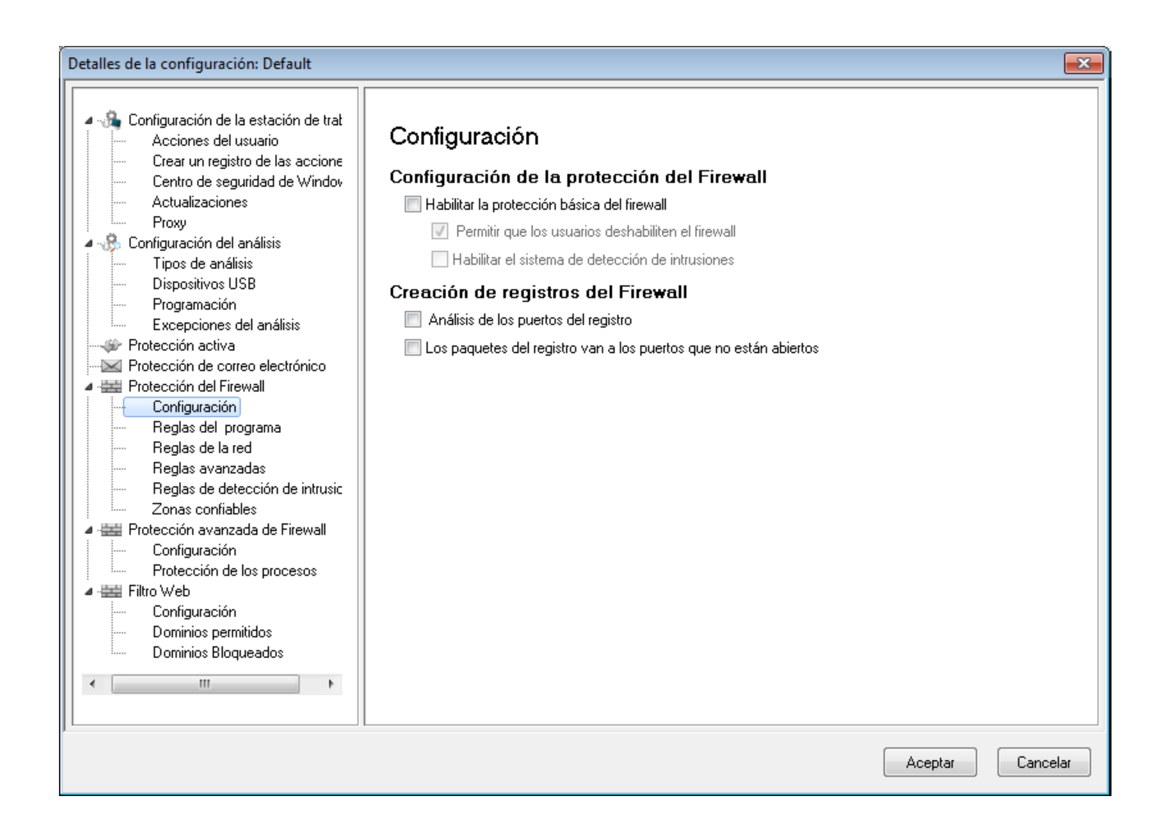
- *Habilitar protección de correo electrónico*: active esta casilla de verificación para habilitar la protección de correo electrónico. Las siguientes opciones estarán disponibles si se activa *Habilitar protección de correo electrónico*:
  - — *Habilitar protección para Outlook:* active esta casilla de verificación para habilitar la protección para Outlook. Faronics Anti-Virus analizará todos los correos electrónicos entrantes y salientes en Outlook.
  - — *Habilitar protección para Outlook Express/Windows Mail:* active esta casilla de verificación para habilitar la protección para Outlook Express/Windows Mail. Faronics Anti-Virus analiza todos los mensajes de correo electrónico entrantes y salientes de Outlook/Windows Mail.
  - — *Habilitar protección para otros clientes de correo electrónico*: especifique la configuración de puerto de correo electrónico para Entrante (POP3) y Saliente (SMTP). Faronics Anti-Virus analiza todos los mensajes de correo electrónico de los programas de correo electrónico con las configuraciones de correo *Entrante* y *Saliente*.



9. Especifique los ajustes en el nodo *Protección de firewall*:

   El nodo Protección de firewall proporciona protección bidireccional, ya que protege el equipo del tráfico entrante y saliente. Puede crear reglas personalizadas para proteger su red. Puede *Permitir* o *Bloquear* la comunicación y también configurar el firewall para que le *Pregunte*.

- *Nodo Firewall*> panel *Configuración*



Configuración de la protección de firewall

— *Habilitar protección de firewall básica*: active esta casilla de verificación para habilitar la protección de firewall.

— *Permitir al usuario deshabilitar el firewall* : esta casilla de verificación se activa al seleccionar *Habilitar protección de firewall básica*. Seleccione esta opción para permitir al usuario deshabilitar el firewall en la estación de trabajo.

— Habilitar sistema de detección de intrusiones: active esta casilla de verificación para habilitar el sistema de detección de intrusiones.

Registro de firewall:

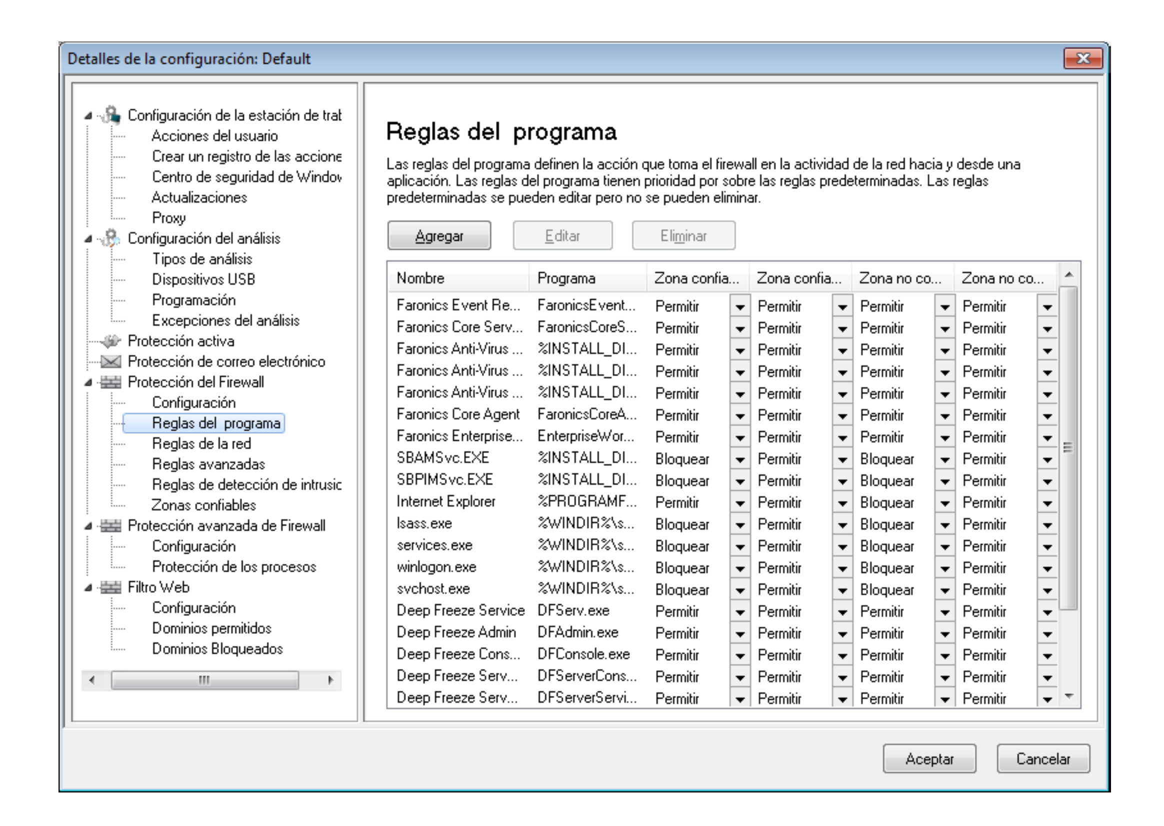
— *Registrar paquetes dirigidos a puertos no abiertos*: active esta casilla de verificación para registrar los paquetes de datos dirigidos a puertos no abiertos. Estos datos proporcionan información útil sobre los intentos de comunicación con puertos no abiertos en la red.

— *Registrar análisis de puertos*: active esta casilla de verificación para registrar todos los intentos de análisis de los puertos de la red. Los datos de análisis de los puertos se guardarán en el archivo de registro.



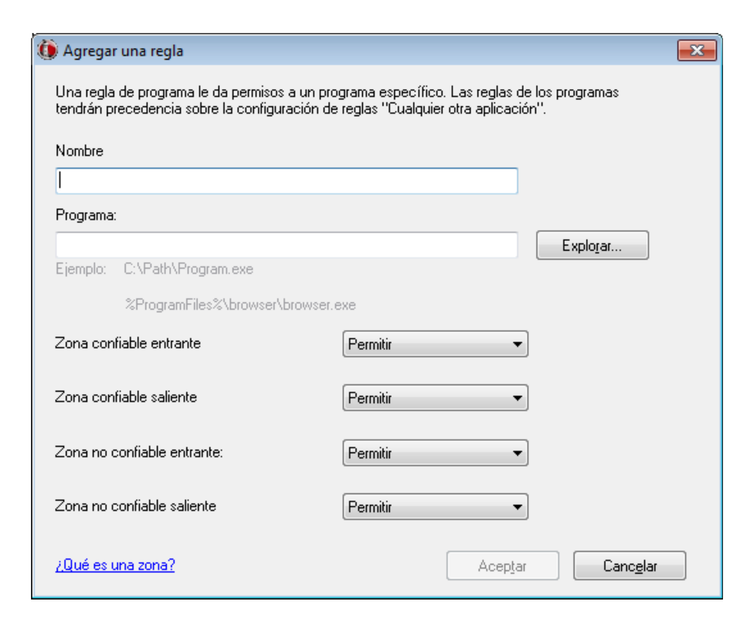
- Nodo *Protección de firewall* > panel *Reglas de programa*

Las reglas de programa definen las acciones que realizará el firewall en relación con la actividad de red hacia y desde una aplicación. Las reglas de programa tienen prioridad sobre las reglas predeterminadas. Las reglas predeterminadas pueden editarse, pero no pueden eliminarse.





Haga clic en *Agregar* para agregar una regla de programa. Especifique o seleccione las opciones correspondientes y haga clic en *Aceptar*. Se mostrarán los parámetros siguientes:



— *Nombre*: nombre de la regla.

— *Programa*: nombre del programa, incluidas su extensión y ruta completa.

— Zona de confianza (Entrada): la acción que se realizará para las comunicaciones entrantes dirigidas al programa en una zona de confianza (*Permitir*, *Bloquear* o *Preguntar*).

— Zona de confianza (Salida): la acción que se realizará para las comunicaciones salientes procedentes del programa en una zona de confianza (*Permitir*, *Bloquear* o *Preguntar*).

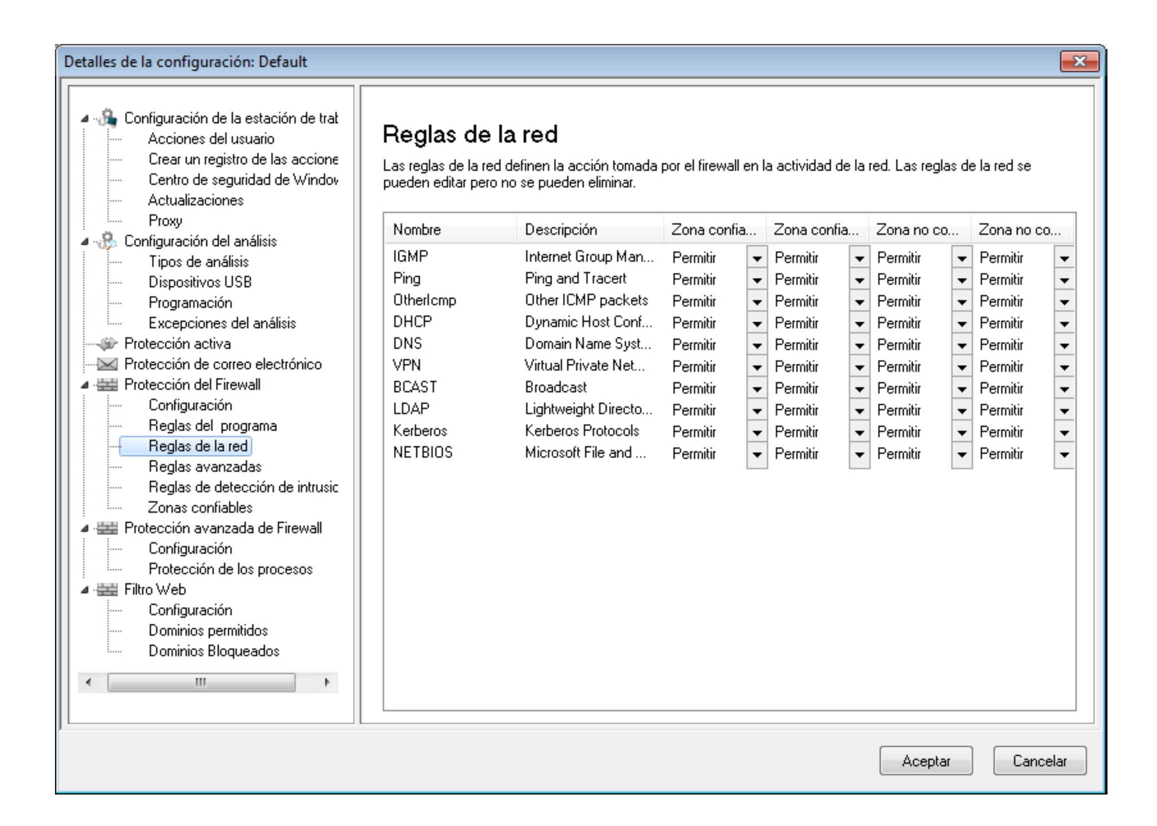
— Zona de no confianza (Entrada): la acción que se realizará para las comunicaciones entrantes dirigidas al programa en una zona de no confianza (*Permitir*, *Bloquear* o *Preguntar*).

— Zona de no confianza (Salida): la acción que se realizará para las comunicaciones salientes procedentes del programa en una zona de no confianza (*Permitir*, *Bloquear* o *Preguntar*).



- Nodo *Protección de firewall* > panel *Reglas de red*

Las reglas de red definen las medidas que tomará el firewall en relación con la actividad de red. Las reglas de red pueden editarse pero no eliminarse.



Se mostrarán los parámetros siguientes:

— *Nombre*: nombre del protocolo.

— *Descripción*: descripción del protocolo.

— Zona de confianza (Entrada): la acción que se realizará para las comunicaciones entrantes dirigidas al protocolo en una zona de confianza (*Permitir*, *Bloquear* o *Preguntar*).

— Zona de confianza (Salida): la acción que se realizará para las comunicaciones salientes procedentes del protocolo en una zona de confianza (*Permitir*, *Bloquear* o *Preguntar*).

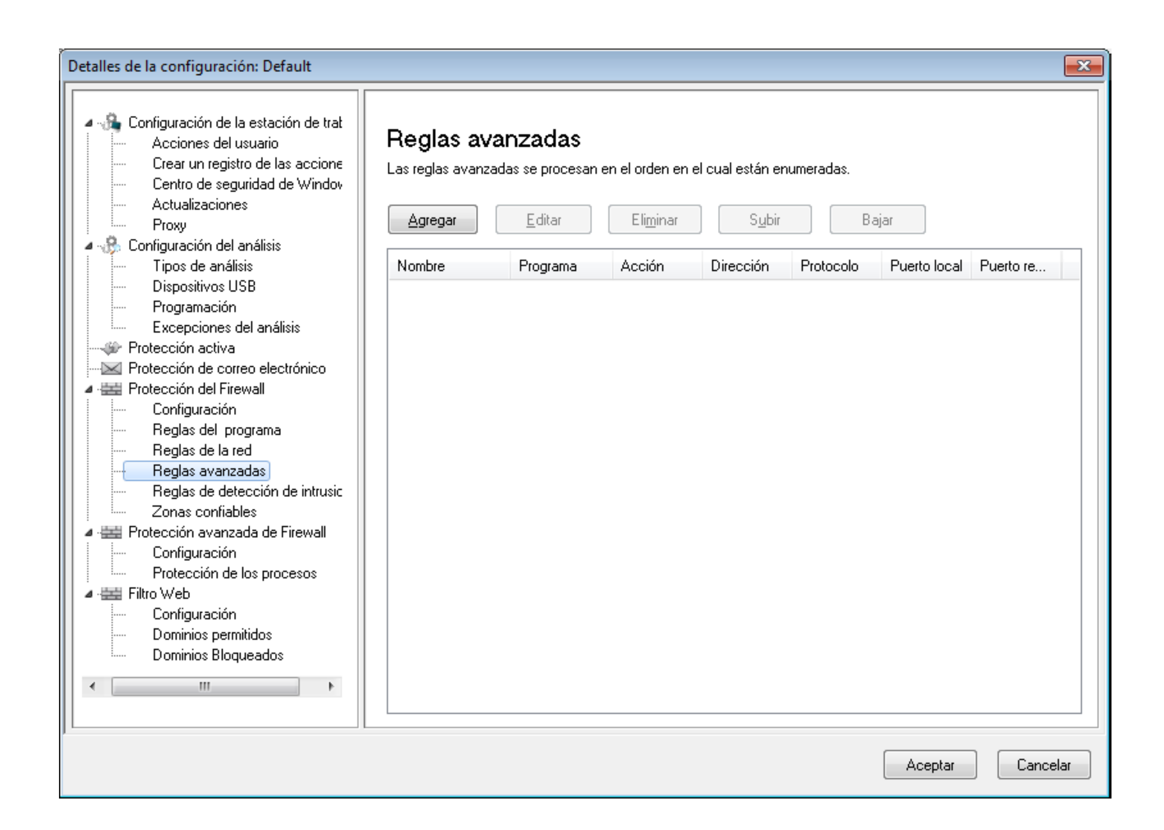
— Zona de no confianza (Entrada): la acción que se realizará para las comunicaciones entrantes dirigidas al protocolo en una zona de no confianza (*Permitir*, *Bloquear* o *Preguntar*).

— Zona de no confianza (Salida): la acción que se realizará para las comunicaciones salientes procedentes del protocolo en una zona de no confianza (*Permitir*, *Bloquear* o *Preguntar*).



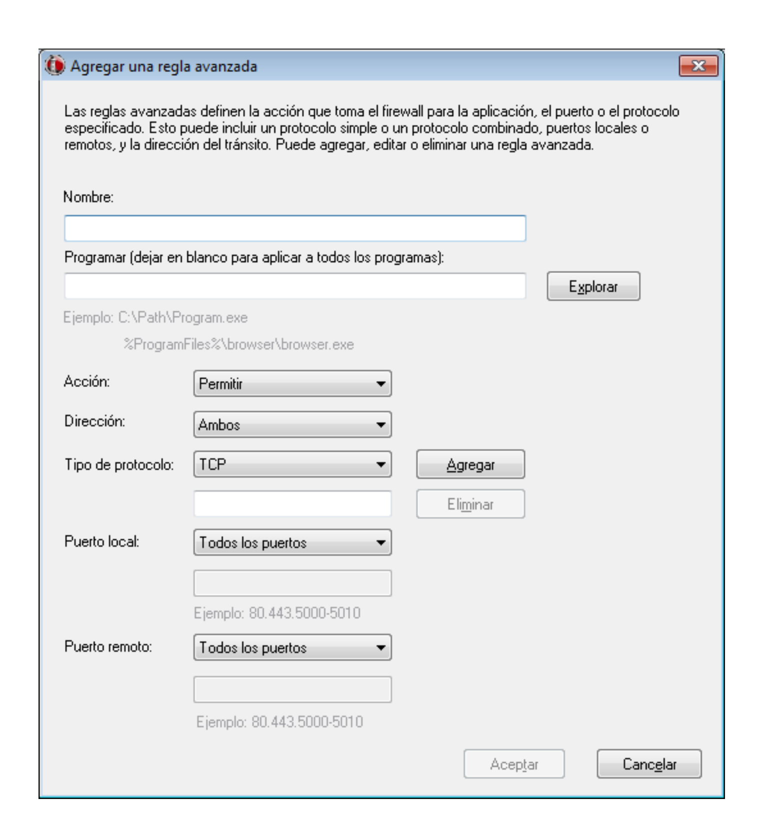
- Nodo *Protección de firewall* > panel *Reglas avanzadas*

Las reglas avanzadas definen las medidas que tomará el firewall en relación con una aplicación, puerto o protocolo especificados. Esto puede incluir un solo protocolo o una combinación de protocolo, puertos locales o remotos y dirección de tráfico. Puede agregar, editar o eliminar una regla avanzada.



Haga clic en *Agregar* para agregar una regla avanzada. Especifique o seleccione las opciones correspondientes y haga clic en *Aceptar*. El panel Reglas avanzadas incluye los parámetros siguientes:





— *Nombre*: nombre de la regla.

— *Programa*: nombre y ruta del programa.

— *Acción*: la acción que realizará el firewall para las comunicaciones procedentes de la aplicación, puerto o protocolo especificados (*Permitir*, *Bloquear* o *Preguntar*).

— *Dirección*: la dirección de la comunicación (*Ambas*, *Hacia dentro o Hacia fuera*).

— *Protocolo*: el nombre del protocolo.

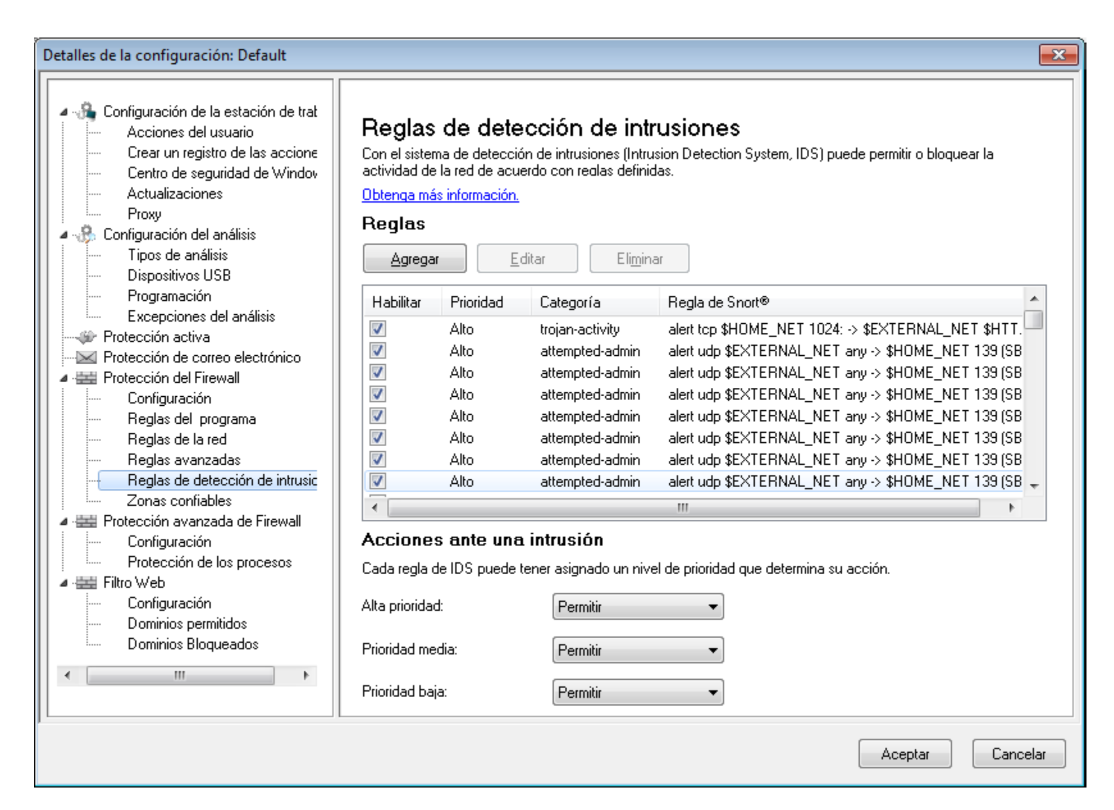
— *Puerto local*: ajustes del puerto local.

— *Puerto remoto*: ajustes del puerto remoto.

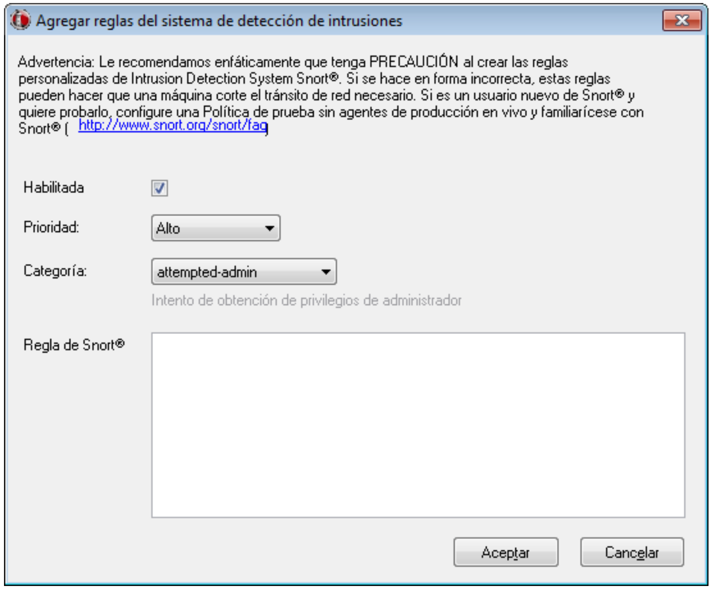


- Nodo *Protección de firewall* >panel *Reglas de detección de intrusiones*

El sistema de detección de intrusiones (Intrusion Detection System, IDS) permite autorizar o bloquear la actividad de red según las reglas de detección de intrusiones definidas. Especifique la acción (Permitir o Bloquear) en el panel Reglas de detección de intrusiones para cada regla. Haga clic en *Editar* o *Eliminar* para editar o eliminar una regla preexistente.



Haga clic en *Agregar* para agregar una regla de detección de intrusiones. Especifique o seleccione las opciones correspondientes y haga clic en *Aceptar*. Al hacer clic en *Agregar*, se mostrarán los parámetros siguientes:



— *Habilitado*: seleccione si es preciso habilitar una regla.

— *Prioridad*: seleccione si la prioridad debe ser *Alta*, *Media* o *Baja*.

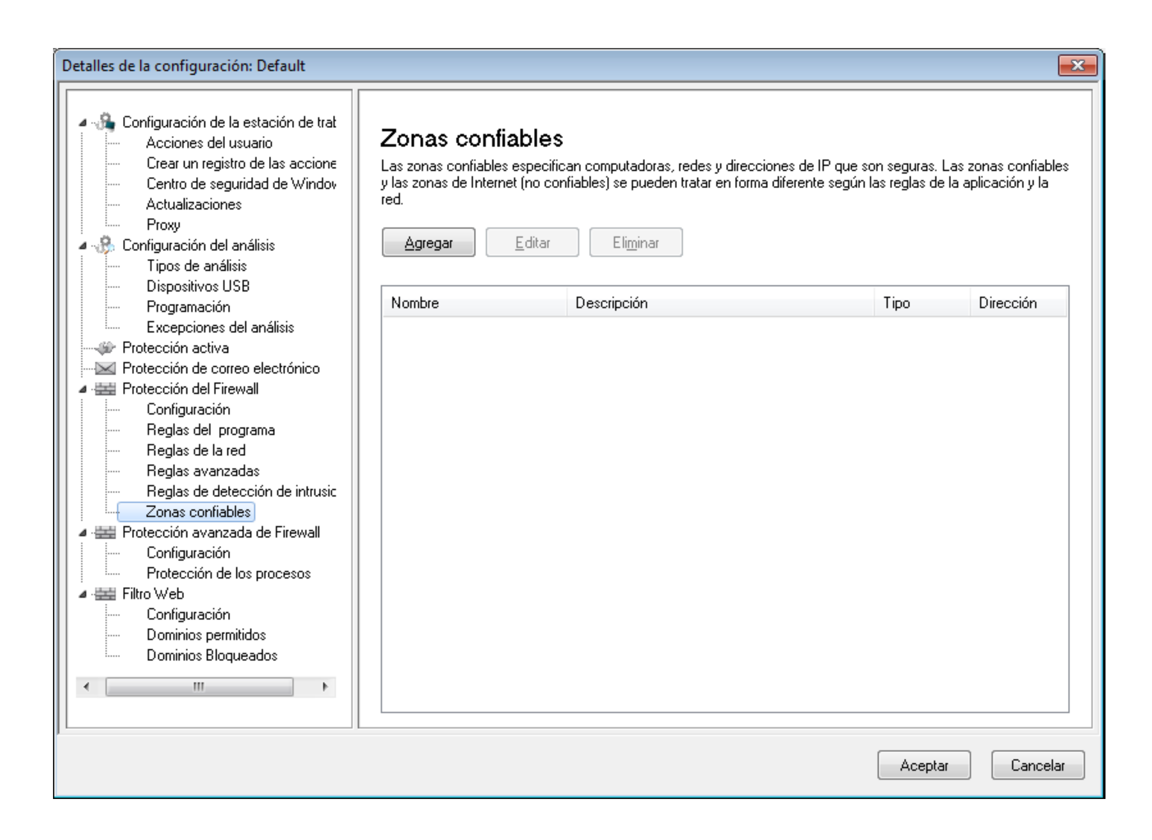
— *Categoría*: seleccione la categoría correspondiente (como *bad-unknown*, *attempted-admin, attempted-dos o attempted-recon*).

— *Regla Snort*: especifique una regla Snort. Para obtener más información sobre las reglas Snort, visite www.snort.org/snort/faq.

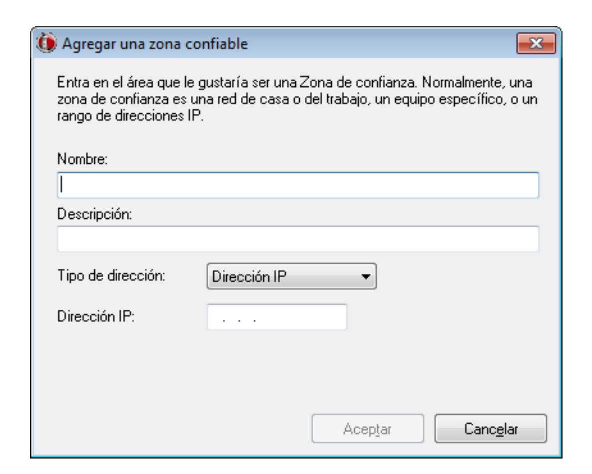
- Nodo *Protección de firewall* > panel *Zonas de confianza*

Las zonas de confianza especifican equipos, redes y direcciones IP seguros. Es posible tratar las zonas de confianza e Internet (zona de no confianza) de forma distinta mediante reglas de red y de programa.





Haga clic en *Agregar* para agregar una zona de confianza. Especifique o seleccione las opciones correspondientes y haga clic en *Aceptar*. Se mostrarán los parámetros siguientes:



— *Nombre*: nombre de la zona de confianza.

— *Descripción*: descripción de la zona de confianza.

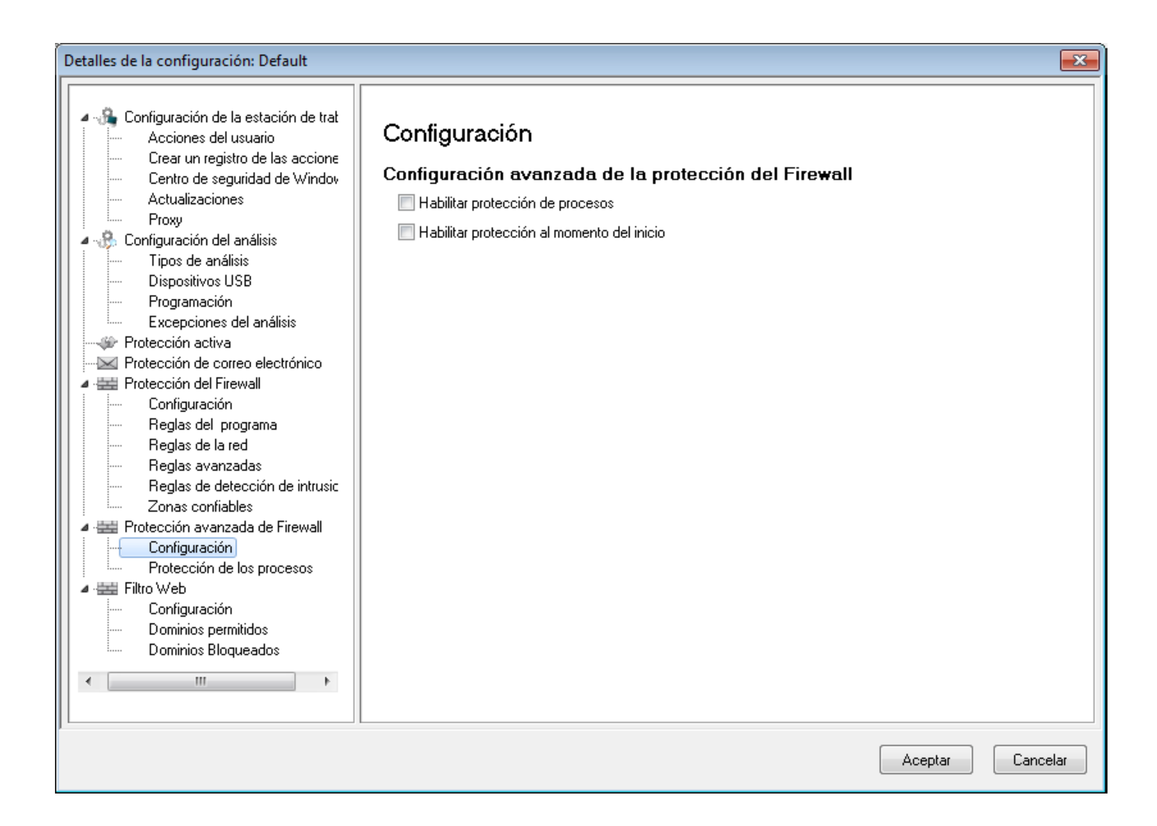
— *Tipo*: tipo de zona de confianza (*Dirección IP*, *Intervalo de direcciones* o *Red*).

10. Especifique los ajustes en el nodo Protección de firewall avanzada:

- Nodo *Protección del Firewall avanzada* > panel *Configuración*



El panel Configuración permite habilitar o deshabilitar la protección de procesos y la protección al inicio.



Seleccione las opciones y haga clic en *Aplicar*. Se mostrarán los parámetros siguientes:

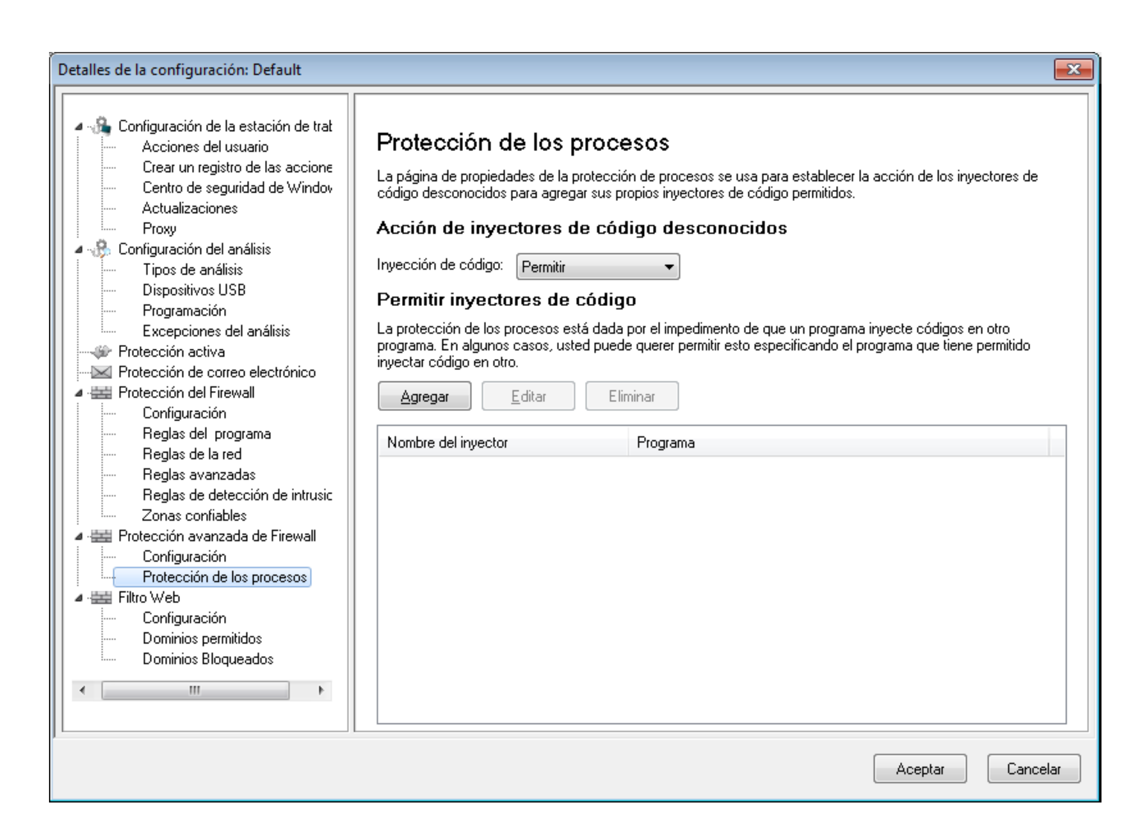
— *Habilitar protección de procesos*: seleccione esta opción para habilitar la protección de procesos. Esta función se utiliza para establecer la acción para los inyectores de código desconocidos y para agregar inyectores de código permitidos de acuerdo con la configuración especificada en el panel *Protección de procesos*.

— *Habilitar protección al inicio*: seleccione esta opción para habilitar la protección al inicio. La protección al inicio protege el equipo cuando se inicia bloqueando el tráfico antes de que Windows pueda abrirlo.

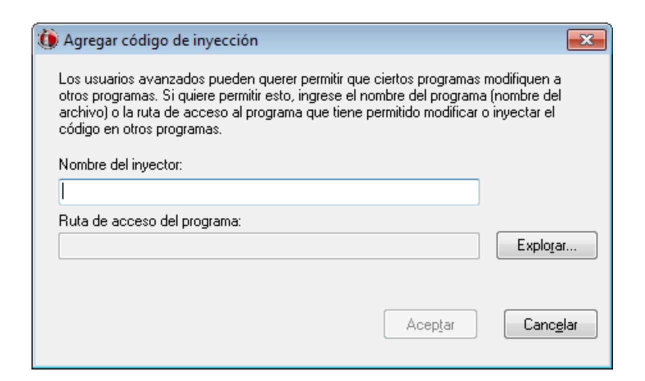
- Nodo *Protección de firewall* > panel *Protección de procesos*

La página de propiedades de protección de procesos permite agregar inyectores de códigos permitidos y establecer la acción que tendrá lugar cuando se detecten inyectores de código desconocidos. La protección de procesos evita que un programa inyecte código a otro programa. Sin embargo, esto puede ser deseable en ocasiones. En tal caso, especifique el programa que tenga permitido inyectar código a otro.





Haga clic en *Agregar* para agregar un inyector de código. Especifique o seleccione las opciones correspondientes y haga clic en *Aceptar*. Se mostrarán los parámetros siguientes:



— *Nombre de inyector*: especifique el nombre del inyector.

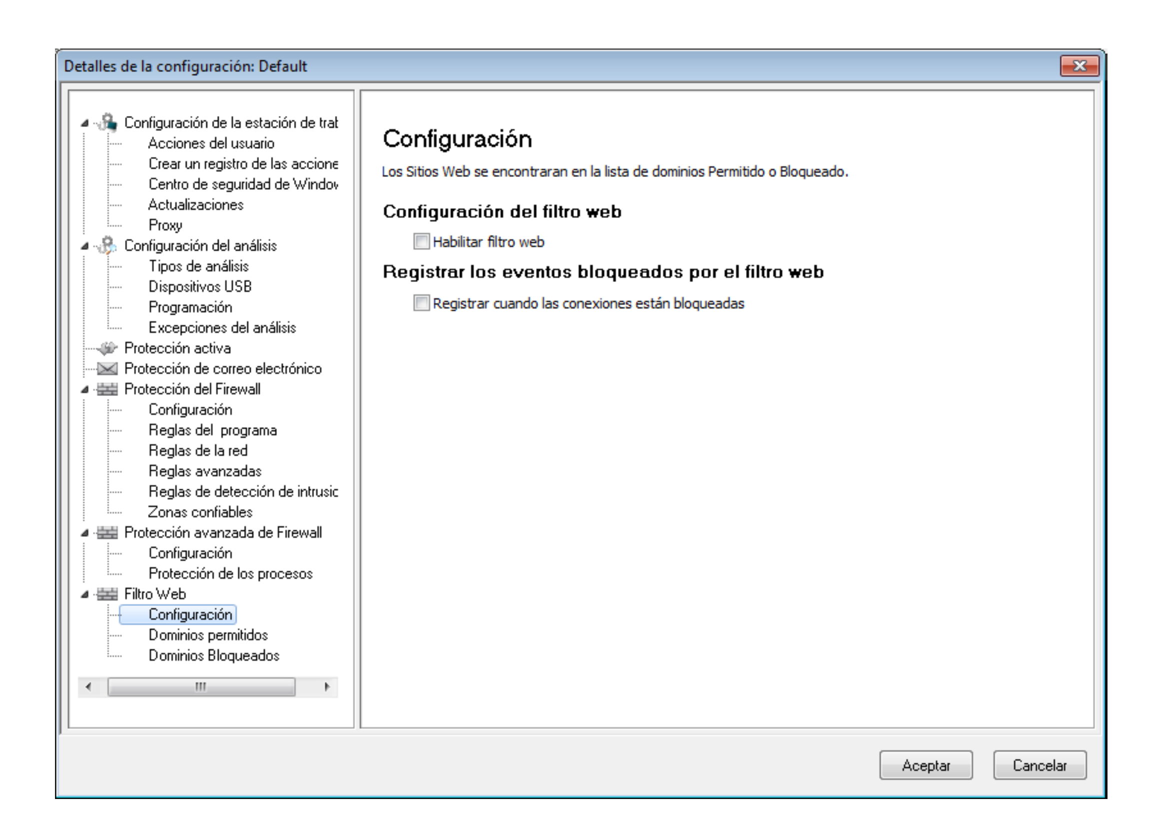
— *Ruta de programa*: seleccione la ruta del programa.

11. Especifique los ajustes en el nodo Filtro web.

- Nodo *Filtro web* > panel *Configuración*

El filtro web evita que se muestre cierto tipo de información en el explorador. Este panel permite establecer la configuración predeterminada para el filtro web.



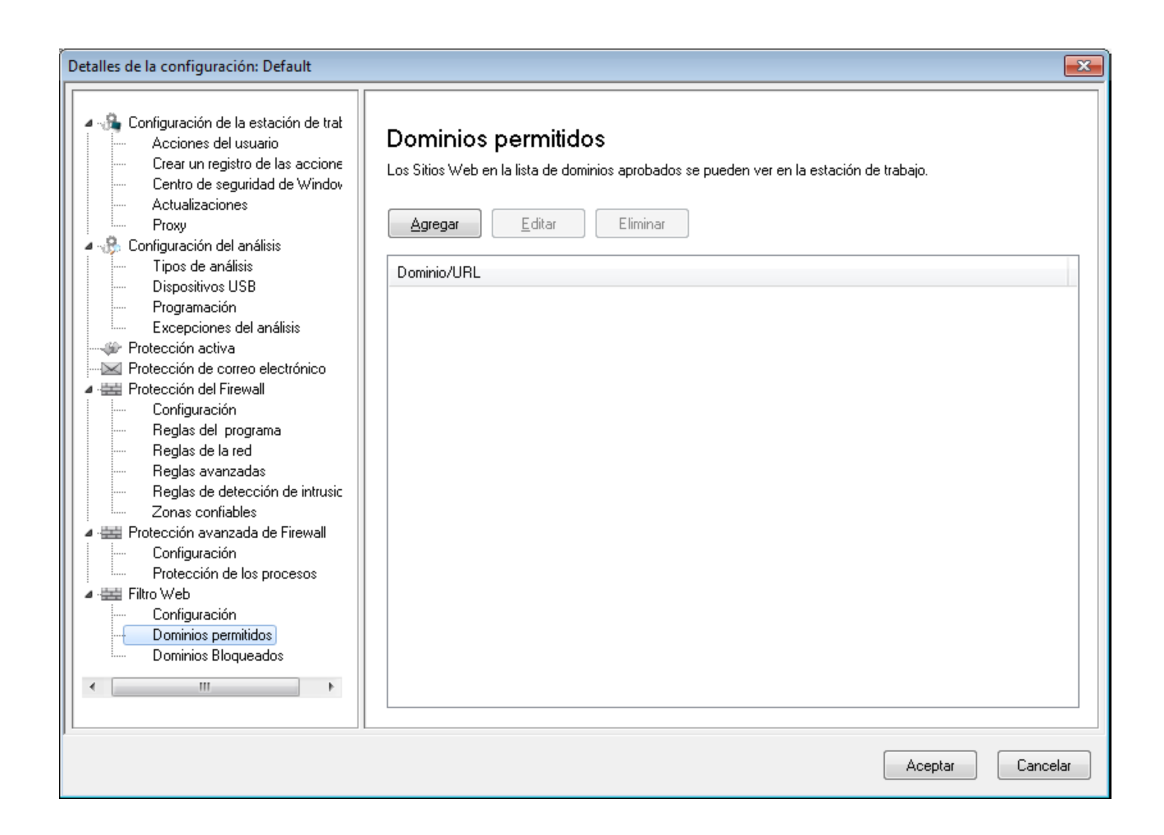


- Seleccione *Habilitar filtro web* para habilitar esta función.
- Seleccione *Registrar bloqueo de conexiones* para que la acción realizada por Faronics Anti-Virus se registre en el archivo de registro.

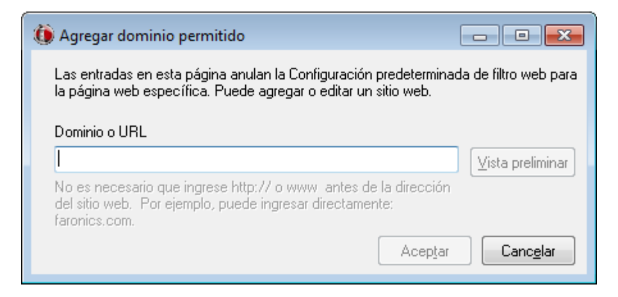


- Nodo *Filtro web* > panel *Dominios permitidos*

Dominios permitidos anula la configuración de filtro web predeterminada y los sitios web agregados a la lista de anuncios bloqueados.



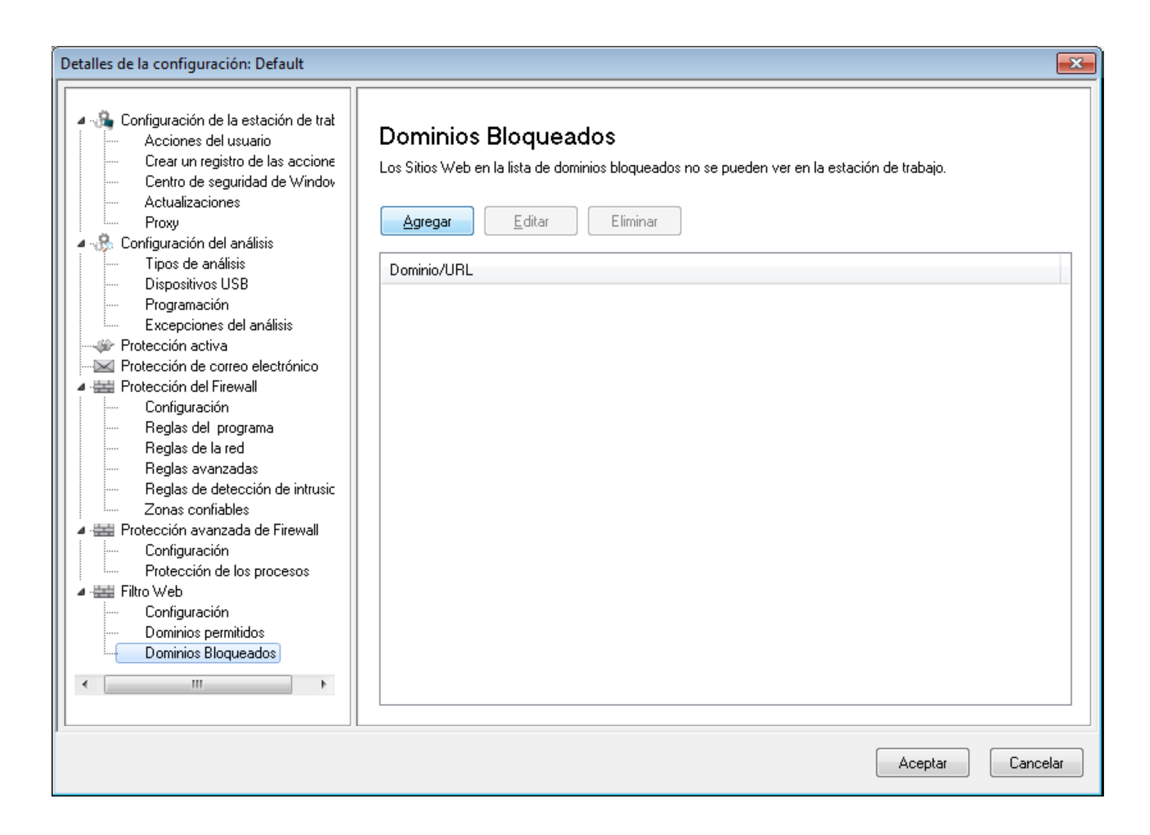
Haga clic en *Agregar* para agregar un dominio permitido. Especifique o seleccione las opciones correspondientes y haga clic en *Aceptar*. Se mostrarán los parámetros siguientes:



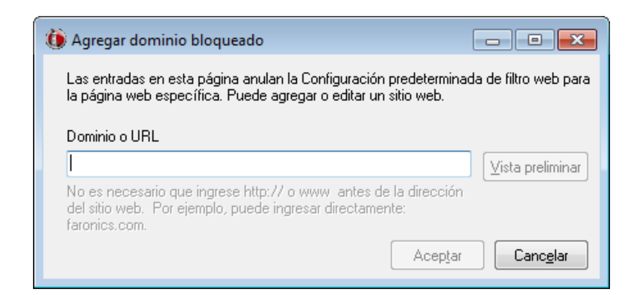
- Dominio o URL: especifique el dominio o la URL que se permitirán. Haga clic en Vista preliminar para ver una vista preliminar del dominio o URL.
- Nodo *Filtro web* > panel *Dominios bloqueados*

Especifique los dominios que se deben bloquear en la red.





Haga clic en *Agregar* para agregar un dominio bloqueado. Especifique o seleccione las opciones correspondientes y haga clic en *Aceptar*. Se mostrarán los parámetros siguientes:



- Dominio o URL: especifique el dominio o la URL que se permitirán. Haga clic en Vista preliminar para ver una vista preliminar del dominio o URL.

12. Haga clic en *Aceptar*.
13. Especifique el nombre de la configuración y haga clic en *Aceptar*.

Aplicación de la configuración de Anti-Virus

Siga los pasos descritos a continuación para aplicar la configuración de Anti-Virus:

1. Vaya al panel *Estaciones de trabajo*.
2. Seleccione una o más estaciones de trabajo.



3. Haga clic con el botón secundario en una o más estaciones de trabajo y seleccione *Actualizar configuración > Anti-Virus > [Nombre de la configuración]*.

La configuración se aplicará a las estaciones de trabajo seleccionadas.



Los cambios en la configuración se aplicarán automáticamente a las estaciones de trabajo en línea. Si las estaciones de trabajo están desconectadas, los cambios en la configuración se aplicarán cuando las estaciones de trabajo se vuelvan a conectar.

Edición de la configuración de Anti-Virus

Siga los pasos descritos a continuación para editar la configuración de Anti-Virus:

1. Vaya al panel Red y grupos en la consola Enterprise.
2. Seleccione *Configuraciones disponibles > Anti-Virus > [Nombre de la configuración]*.
3. Haga clic con el botón secundario en la configuración seleccionada y seleccione *Editar configuración seleccionada*.
4. Edite la configuración según sea necesario.
5. Haga clic en *Aceptar*.

Eliminación de una configuración de Anti-Virus

Siga los pasos descritos a continuación para eliminar la configuración de Anti-Virus:

1. Vaya al panel Red y grupos en la consola Enterprise.
2. Seleccione *Configuraciones disponibles > Anti-Virus > [Nombre de la configuración]*.
3. Haga clic con el botón secundario en la configuración seleccionada y seleccione *Eliminar configuración seleccionada*.
4. Haga clic en *Aceptar*.



Usar Faronics Anti-Virus desde la consola Enterprise

Una vez que el cliente de Faronics Anti-Virus esté instalado en la estación de trabajo, se pueden realizar varias acciones en la estación de trabajo a través de la consola Deep Freeze.

Comandos de Anti-Virus

Existen dos formas para aplicar los mismos comandos a través de la consola Deep Freeze:

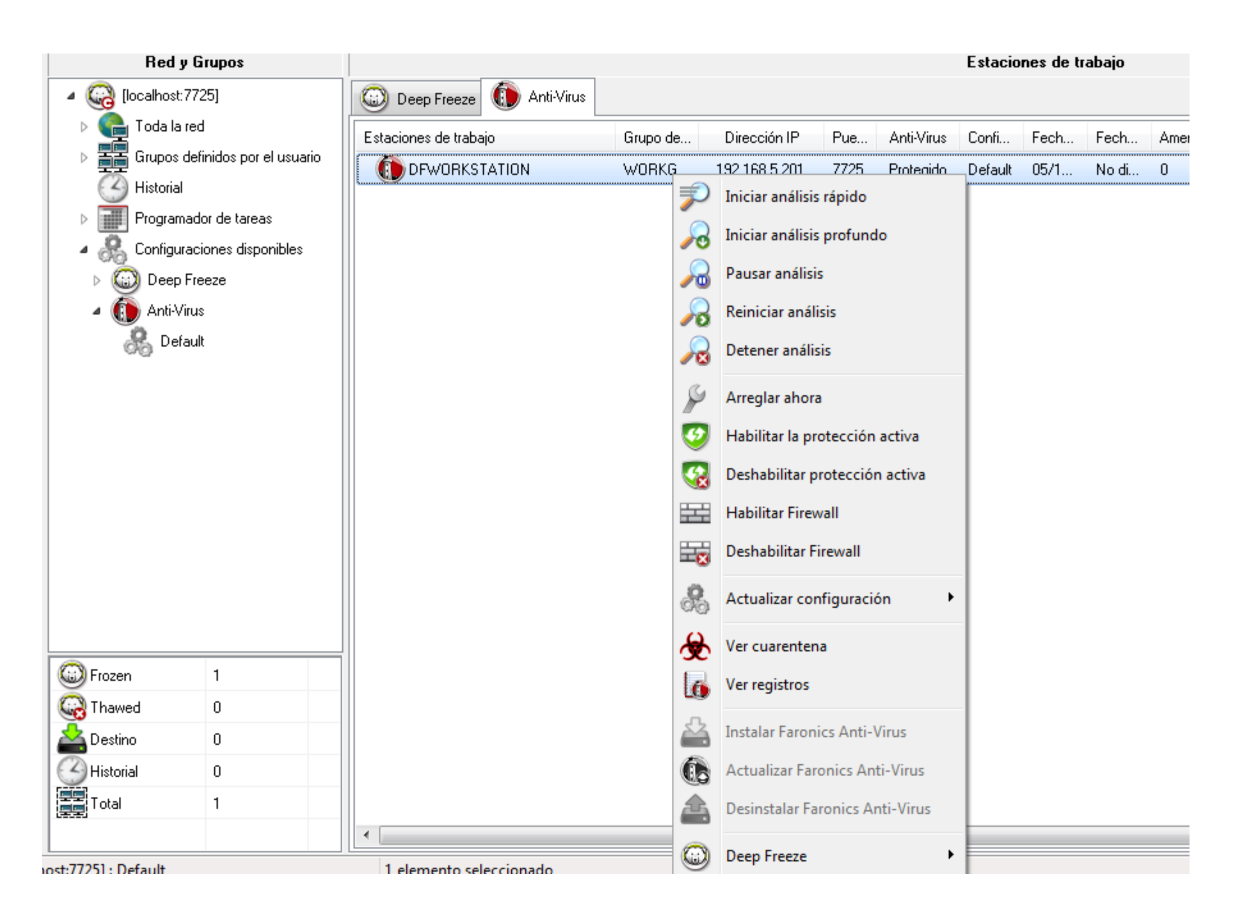
- Menú Anti-Virus (en la barra de menús)
- Menú contextual de Anti-Virus (clic con el botón secundario en el menú contextual)

Los comandos del menú se explicarán en más detalle en esta sección.

Los siguientes comandos están disponibles en el menú Anti-Virus.



Los mismos comandos están disponibles en el panel *Estaciones de trabajo* > ficha *Anti-Virus* > menú contextual:





Análisis rápido

El análisis rápido analiza las áreas comúnmente afectadas de su equipo. Su duración es menor que el análisis a fondo del sistema. El análisis rápido también usa menos memoria que el análisis a fondo del sistema.

— Para iniciar un análisis rápido

Seleccione una o más estaciones de trabajo. Haga clic con el botón secundario y seleccione *Iniciar análisis rápido*.

— Para detener un análisis rápido

Seleccione una o más estaciones de trabajo. Haga clic con el botón secundario y seleccione *Detener análisis*.

— Para pausar un análisis rápido

Seleccione una o más estaciones de trabajo. Haga clic con el botón secundario y seleccione *Pausar análisis*.

— Para reanudar un análisis rápido

Seleccione una o más estaciones de trabajo. Haga clic con el botón secundario y seleccione *Reanudar análisis*.

Análisis a fondo

El análisis a fondo del sistema realiza un análisis minucioso de todas las áreas del equipo. La duración del análisis dependerá del tamaño de la unidad de disco duro.

— Para iniciar un análisis a fondo

Seleccione una o más estaciones de trabajo. Haga clic con el botón secundario y seleccione *Iniciar análisis a fondo*.

— Para detener un análisis a fondo

Seleccione una o más estaciones de trabajo. Haga clic con el botón secundario y seleccione *Detener análisis a fondo*.

— Para pausar un análisis a fondo

Seleccione una o más estaciones de trabajo. Haga clic con el botón secundario y seleccione *Pausar análisis*.

— Para reanudar un análisis a fondo

Seleccione una o más estaciones de trabajo. Haga clic con el botón secundario y seleccione *Reanudar análisis*.

Corregir ahora

La opción Corregir ahora descarga las últimas definiciones de virus y realiza un análisis rápido en la estación de trabajo.

— Para Corregir ahora

Seleccione una o más estaciones de trabajo. Haga clic con el botón secundario y seleccione *Corregir ahora*.



Protección activa

La protección activa (Active Protection, AP) es un método de detección de malware en tiempo real. La protección activa funciona en segundo plano mientras trabaja o navega por Internet efectuando un seguimiento permanente de los archivos que se ejecutan sin sobrecargar el sistema.

— Para habilitar la protección activa

Seleccione una o más estaciones de trabajo. Haga clic con el botón secundario y seleccione *Habilitar protección activa*.

— Para deshabilitar la protección activa

Seleccione una o más estaciones de trabajo. Haga clic con el botón secundario y seleccione *Deshabilitar protección activa*.

Firewall

Un firewall proporciona protección bidireccional, ya que protege el equipo del tráfico entrante y saliente. Un firewall protege la red de intrusiones no autorizadas.

— Para habilitar el firewall

Seleccione una o más estaciones de trabajo. Haga clic con el botón secundario y seleccione *Habilitar firewall*.

— Para deshabilitar el firewall

Seleccione una o más estaciones de trabajo. Haga clic con el botón secundario y seleccione *Deshabilitar firewall*.

Enviar mensaje

La opción Enviar mensaje permite enviar un mensaje a las estaciones de trabajo en línea.

— Para enviar un mensaje

Seleccione una o más estaciones de trabajo. Haga clic con el botón secundario y seleccione *Enviar mensaje*.

Acceder a la información de cuarentena

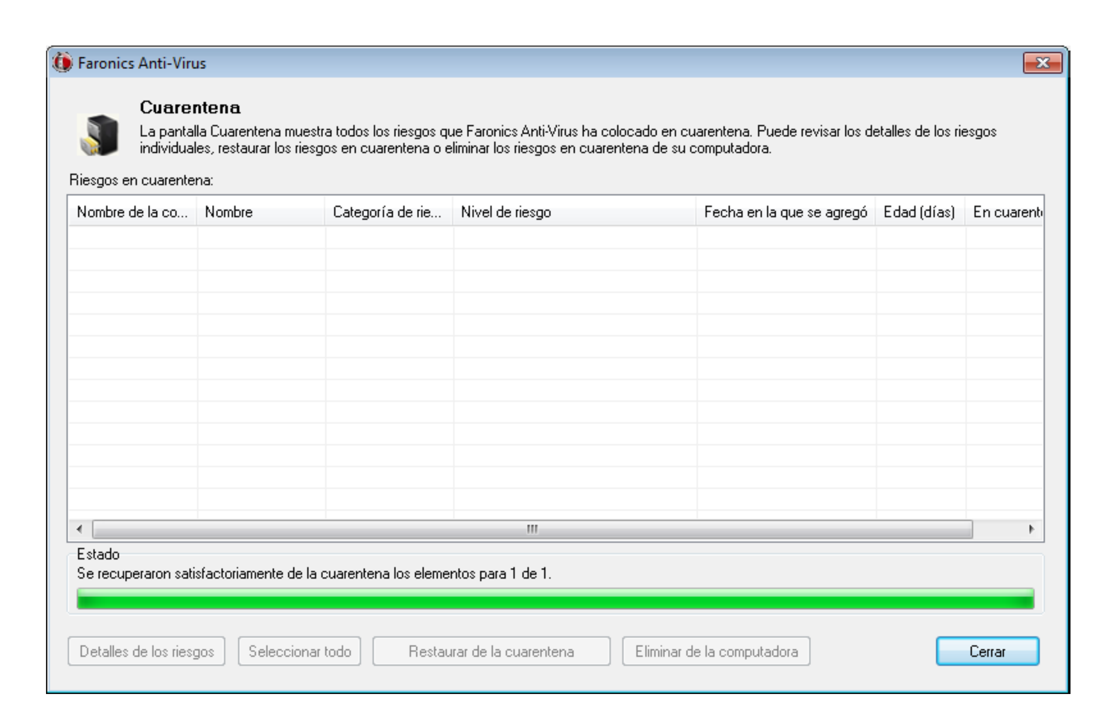
La cuarentena es un lugar seguro en el equipo en el que Faronics Anti-Virus almacena malware y otros archivos infectados que no ha podido desinfectar. Si el equipo o los archivos en el equipo no tienen un comportamiento normal después de que se haya puesto un elemento en cuarentena, podrá consultar la información sobre riesgo, obtener más detalles y quitarlo de la



cuarentena restaurándolo en su ubicación original en el equipo. También puede eliminar de forma permanente los riesgos en cuarentena.

— Para ver la información de cuarentena

Seleccione una o más estaciones de trabajo. Haga clic con el botón secundario y seleccione *Faronics Anti-Virus > Obtener información en cuarentena*.



Acceder a la información de registro

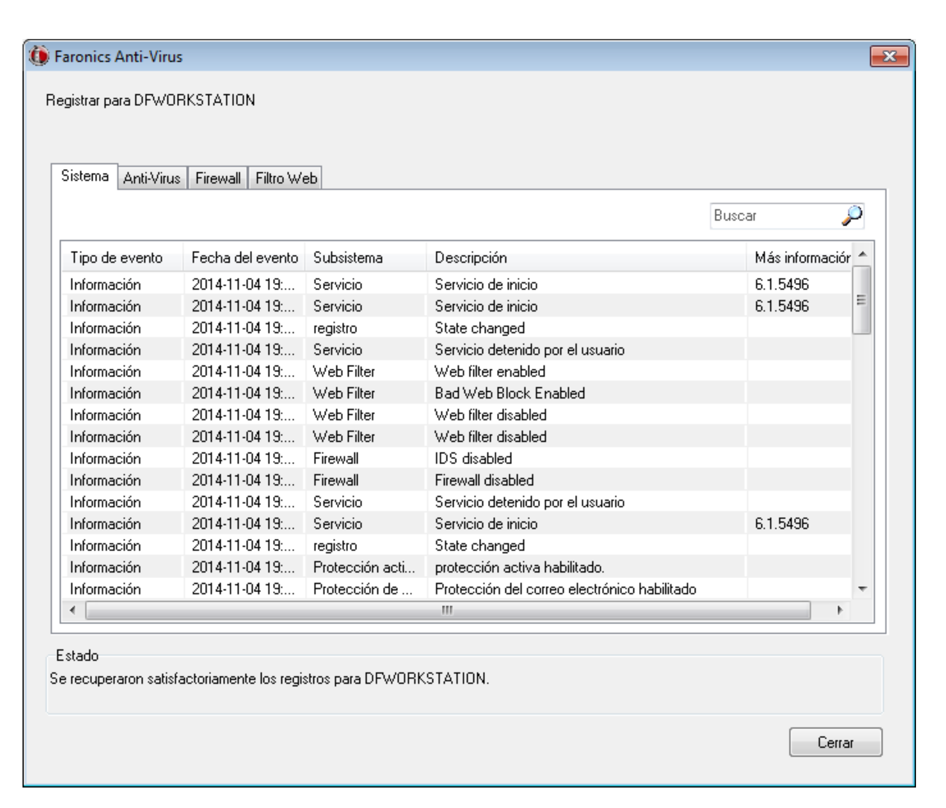
El registro de Faronics Anti-Virus muestra todas las tareas realizadas por Faronics Anti-Virus en la estación de trabajo.

— Para ver la información de registro:

Seleccione una estación de trabajo. Haga clic con el botón secundario y seleccione *Faronics Anti-Virus > Ver información de cuarentena*. Se mostrarán las fichas siguientes:

- Ficha Sistema: muestra los eventos del sistema.





- Ficha Anti-Virus: muestra los eventos de Anti-Virus. Seleccione las siguientes opciones del menú desplegable para ver los resultados seleccionados para:
  — Análisis
  — Protección activa
  — Protección de correo electrónico



Faronics Anti-Virus

Registrar para DFWORKSTATION

Sistema | Anti-Virus | Firewall | Filtro Web

Ver: Protección activa

Analizar
Protección activa
Protección de correo electrónico

Buscar

Fecha/Ho | Aplicación

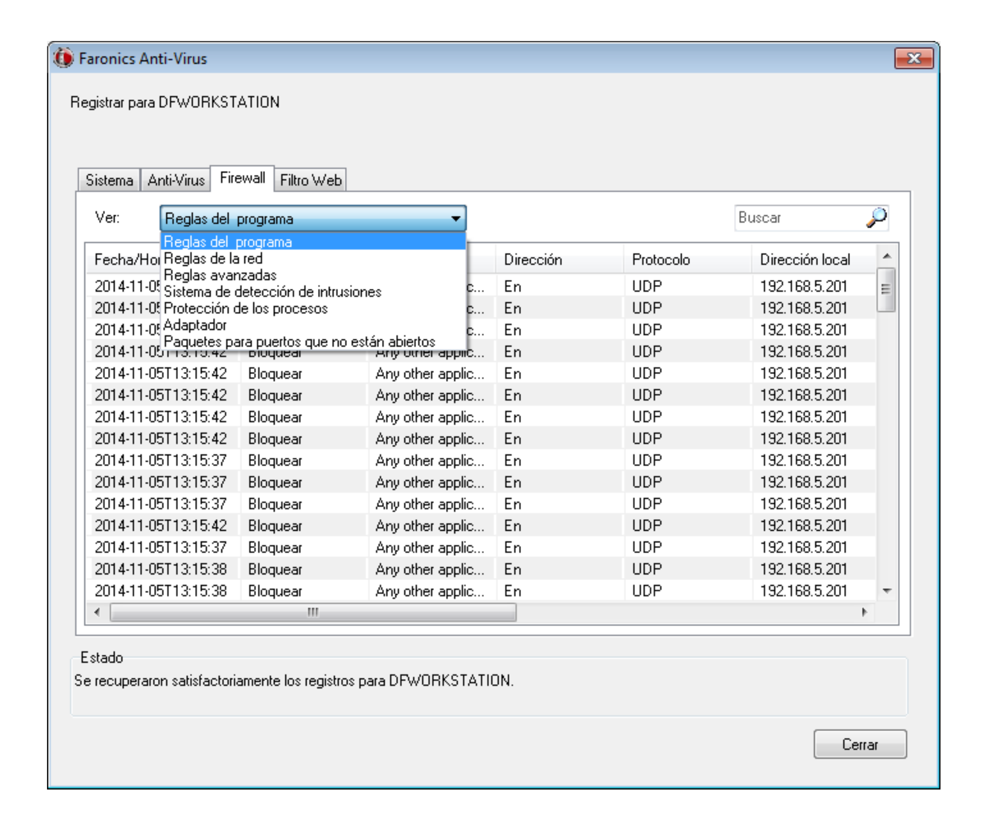
Estado

Se recuperaron satisfactoriamente los registros para DFWORKSTATION.

Cerrar

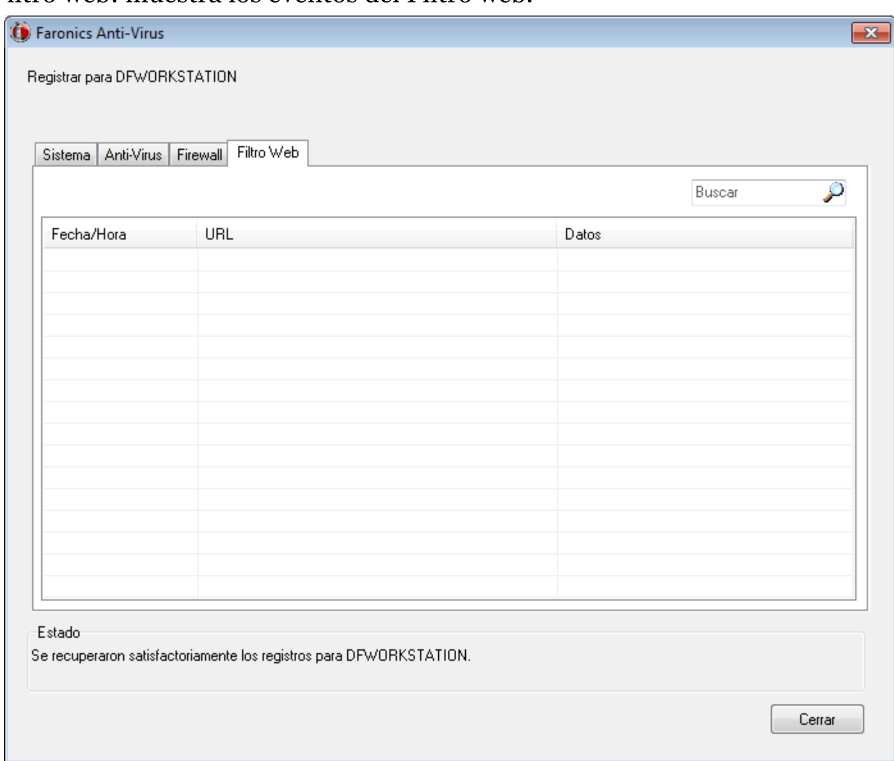


- Ficha Firewall: muestra los eventos del sistema. Busque eventos específicos en el campo Buscar. Seleccione las siguientes opciones del menú desplegable para ver los resultados seleccionados para:
  - — Reglas de programa
  - — Reglas de red
  - — Reglas avanzadas
  - — Sistema de detección de intrusiones
  - — Protección de procesos
  - — Adaptador
  - — Paquetes para puertos que no están abiertos





- Ficha Filtro web: muestra los eventos del Filtro web.





Programar tareas de Anti-Virus

Las siguientes tareas de Anti-Virus se pueden ejecutar desde la consola Deep Freeze de acuerdo con una programación definida previamente.

- Deshabilitar protección activa
- Habilitar protección activa
- Iniciar análisis rápido
- Iniciar análisis a fondo

El procedimiento para programar tareas se explica en detalle en la sección *Programación de tareas de Deep Freeze*.



Usar el cliente de Anti-Virus en la estación de trabajo

Las funciones disponibles en Anti-Virus en la estación de trabajo dependen completamente de los ajustes seleccionados en la configuración de Anti-Virus. Para obtener más información acerca de la configuración de Anti-Virus, consulte *Configuración de Anti-Virus*.

Inicio de Anti-Virus en la estación de trabajo

Vaya a *Inicio>Programas>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. También puede hacer doble clic en el icono de Faronics Anti-Virus en la bandeja de sistema.



Los siguientes paneles muestran información importante para el usuario:

- *Protegido* o *No protegido* aparece para notificar si el equipo está protegido o no. Si aparece No protegido, haga clic en el botón *Corregir ahora* debajo del aviso *No protegido*.
- *Estado de análisis* muestra cuándo se realizó el último análisis. Para analizar ahora, haga clic en el enlace *Analizar ahora*.
- *Estado de actualización* muestra cuándo se realizó la última actualización. Para actualizar las definiciones de virus, haga clic en el enlace *Actualizar todo ahora*.
- *Protección activa* muestra si está habilitada la protección en tiempo real.



- *Protección de correo electrónico* muestra si el correo electrónico está protegido por Faronics Anti-Virus.
- *Protección de Firewall* muestra si la estación de trabajo está protegida por el firewall.
- *Protección de filtro web* aparece si la estación de trabajo está protegida por la función de filtro web de Faronics Anti-Virus.
- *Estadísticas de detención de riesgos* muestra las estadísticas para las acciones que ha realizado Faronics Anti-Virus. Haga clic en *Restablecer contadores* para restablecer los contadores a cero.

Análisis de la estación de trabajo

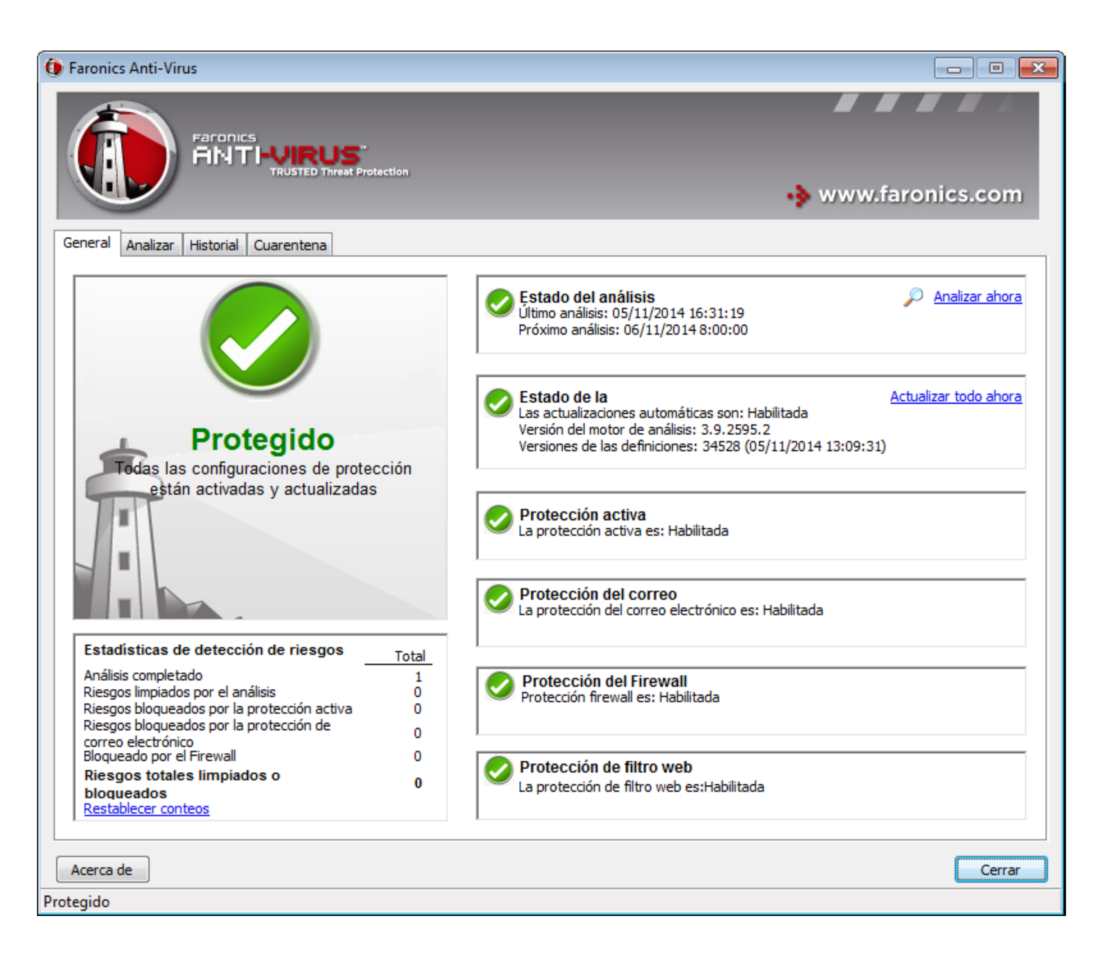
Siga los pasos descritos a continuación para analizar una estación de trabajo:

1. Vaya a *Inicio>Programas>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. También puede hacer doble clic en el icono de Faronics Anti-Virus en la bandeja de sistema.



2. En el panel *Estado de análisis*, haga clic en *Analizar ahora*. Se mostrará la ficha *Analizar*. También puede hacer clic en la ficha *Analizar*.





3. Seleccione una de las opciones siguientes:

- *Análisis rápido*: analiza solo en busca de las amenazas conocidas.
- *Análisis a fondo del sistema*: realiza un análisis minucioso de todos los archivos de la estación de trabajo.
- *Análisis personalizado* (seleccione una de las opciones siguientes):
  - — *Analizar procesos en ejecución*: analiza los procesos en ejecución en la estación de trabajo.
  - — *Analizar registro*: analiza el registro.
  - — *Analizar cookies*: analiza las cookies guardadas en la estación de trabajo.
  - — *Especifique las unidades y carpetas que se analizarán*: Haga clic en *Examinar* para seleccionar las carpetas.

4. Haga clic en *Analizar ahora*. Un icono que gira indica que se está realizando un análisis. Los resultados del análisis se mostrarán una vez finalizado el análisis.
5. Seleccione el archivo y una de las opciones siguientes:

- Seleccione *Cambiar acción de limpieza>Acción recomendada* para realizar la acción recomendada por Faronics Anti-Virus.
- Seleccione *Cambiar acción de limpieza>Poner en cuarentena/Desinfectar* para poner en cuarentena o desinfectar el archivo.
- Seleccione *Cambiar acción de limpieza>Eliminar* para eliminar el archivo.



- Seleccione *Cambiar acción de limpieza>Permitir* para permitir el archivo.
- Haga clic en *Seleccionar todo* para seleccionar todos los archivos que se muestran en *Resultado del análisis*.
- Haga clic en *Detalles* para ver los detalles del riesgo.
- Haga clic en *Cancelar* para cerrar el cuadro de diálogo sin realizar ninguna acción.
- Haga clic en *Limpiar* para eliminar el archivo y cerrar el cuadro de diálogo.

Análisis de un archivo o una carpeta mediante clic con el botón secundario

Es muy fácil comprobar si los archivos o carpetas (uno o varios) tienen virus. Al instalar Faronics Anti-Virus en una estación de trabajo, la opción para analizar en busca de virus se agrega al menú que aparece al hacer clic con el botón secundario.

Realice los siguientes pasos para analizar un archivo o una carpeta en el equipo:

1. Haga clic con el botón derecho en el archivo o carpeta.
2. Seleccione *Analizar en busca de virus*.

Se realizará el análisis y se mostrarán los resultados.

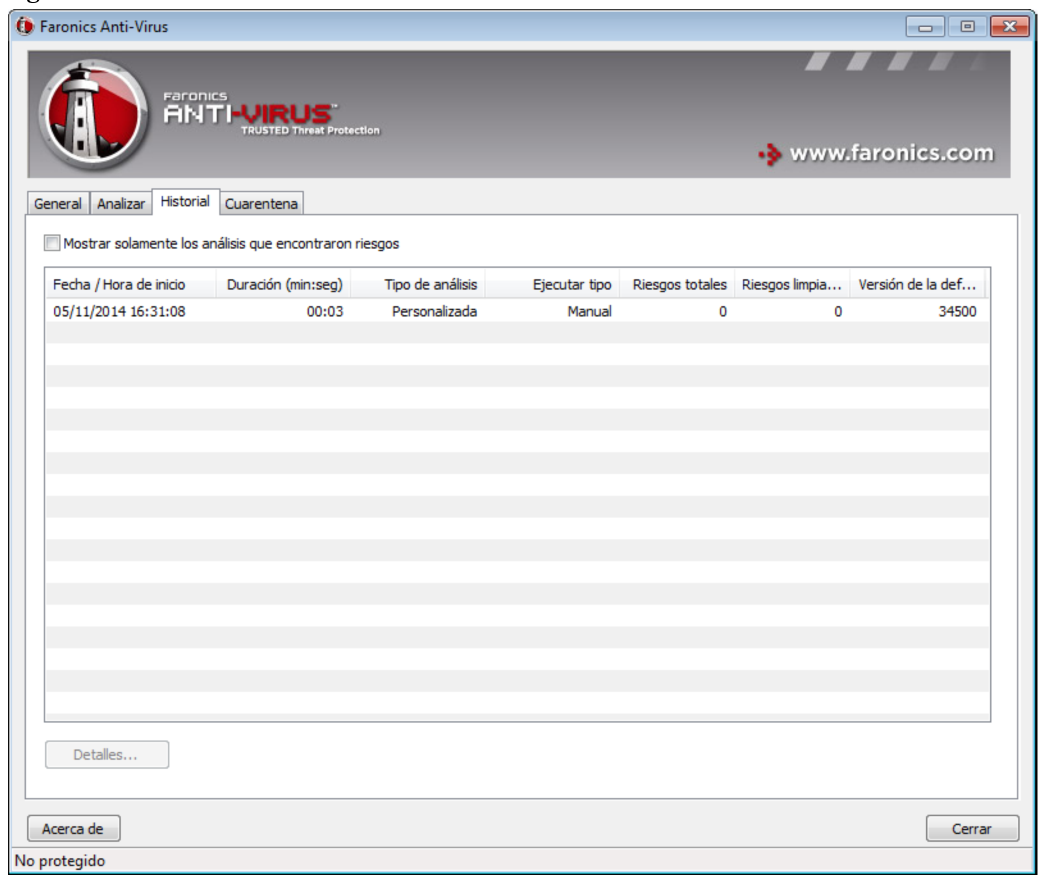
Ver el historial de análisis

Siga los pasos descritos a continuación para ver el historial de análisis:

1. Vaya a *Inicio>Programas>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. También puede hacer doble clic en el icono de Faronics Anti-Virus en la bandeja de sistema.



2. Haga clic en la ficha *Historial*.



3. Seleccione las siguientes acciones:

- *Mostrar solamente análisis con riesgos encontrados*: seleccione esta opción para ver solamente los análisis donde se encuentren riesgos.
- *Detalles*: seleccione una entrada y haga clic en detalles para ver los detalles del análisis.

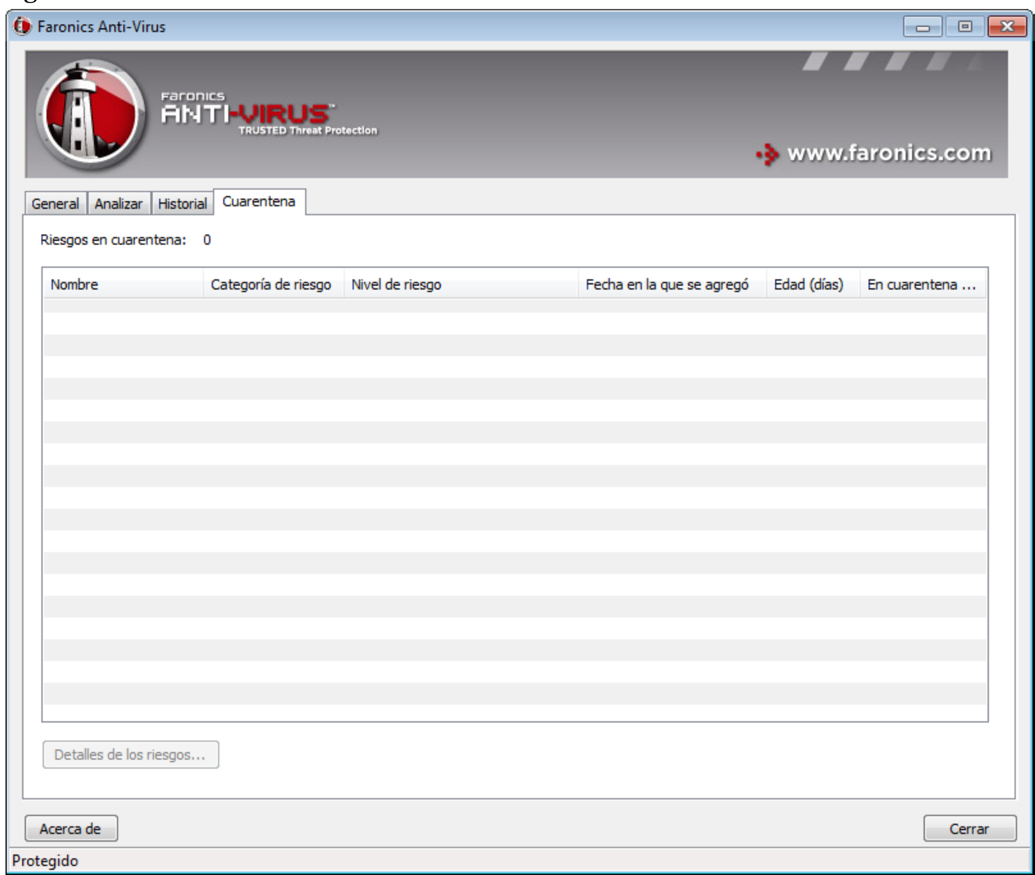
Ver y tomar medidas acerca de los archivos en cuarentena

Siga los pasos descritos a continuación para acceder a Cuarentena:

1. Vaya a *Inicio>Programas>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. También puede hacer doble clic en el icono de Faronics Anti-Virus en la bandeja de sistema.



2. Haga clic en la ficha *Cuarentena*.



3. Haga clic en *Detalles de riesgo*. Se mostrará la siguiente información acerca de cada archivo infectado:

- Nombre
- Categoría de riesgo
- Nivel de riesgo
- Fecha en la que se agregó
- Antigüedad (días)
- Puesto en cuarentena por

4. Seleccione las siguientes acciones:

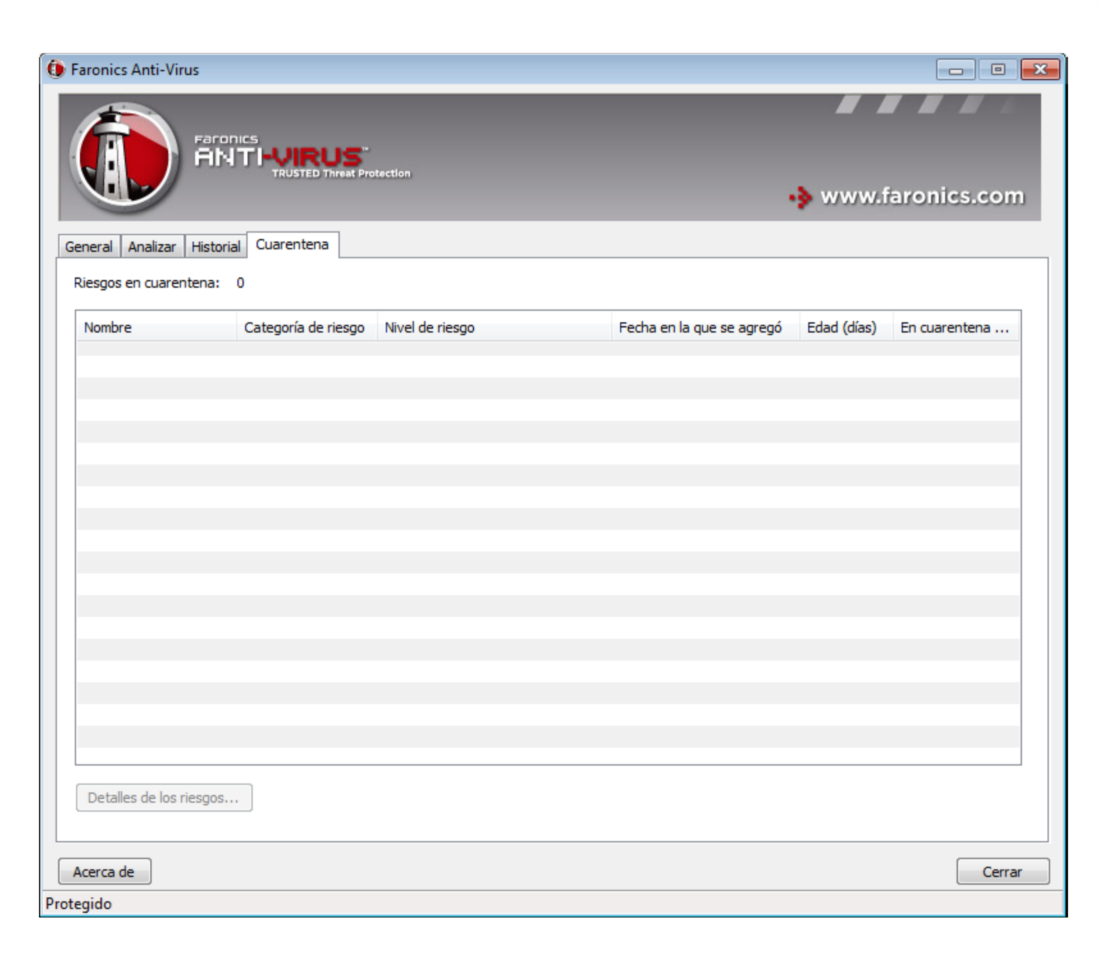
- *Detalles*: seleccione un archivo y haga clic en *Detalles* para ver los detalles del archivo infectado. También se mostrará la acción recomendada.

Actualización de las definiciones de Anti-virus en la estación de trabajo

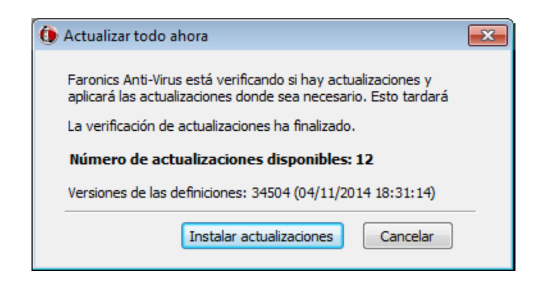
Siga los pasos descritos a continuación para actualizar las definiciones de Anti-Virus en una estación de trabajo:

1. Vaya a *Inicio>Programas>Faronics>Anti-Virus Enterprise>Faronics Anti-Virus Enterprise*. También puede hacer doble clic en el icono de Faronics Anti-Virus en la bandeja de sistema.





2. En el panel *Estado de actualización*, haga clic en *Actualizar todo ahora*. Se mostrará el cuadro de diálogo *Actualizar todo ahora*.



3. Haga clic en *Instalar actualizaciones*. Se actualizarán las definiciones de virus en la estación de trabajo.

Administración de Anti-Virus en la estación de trabajo a través de la bandeja de sistema

Faronics Anti-Virus se puede administrar en la estación de trabajo a través de un menú disponible en la bandeja de sistema.



Haga clic con el botón secundario en el icono de Faronics Anti-Virus en la bandeja de sistema. Estas son las opciones disponibles:

- Abrir Faronics Anti-Virus: inicia Faronics Anti-Virus en la estación de trabajo.
- *Protección activa*
  - *Protección activa>Habilitar protección activa*: habilita la protección activa.
  - *Protección activa>Deshabilitar protección activa> [Seleccione la opción]*: selecciona el tiempo durante el cual la protección activa estará deshabilitada. Seleccione 5 minutos, 15 minutos, 30 minutos, 1 hora, Hasta que el equipo se reinicie o Permanentemente. Esta opción solo se muestra si se ha seleccionado en la directiva de Anti-Virus.
- *Analizar ahora>[Seleccione la opción]*: seleccione Cancelar análisis, Pausar análisis, Reiniciar análisis, Análisis rápido o Análisis a fondo. Esta opción solo se muestra si se ha seleccionado en la directiva de Anti-Virus.
- *Protección de Firewall>Habilitar* o *Deshabilitar*



Comprobar si hay actualizaciones de Anti-Virus

La consola Deep Freeze permite comprobar si hay nuevas versiones disponibles de Faronics Anti-Virus.

Vaya a *Ayuda* > *Buscar actualizaciones*. Se comprobará si hay nuevas versiones de Faronics Anti-Virus disponibles.



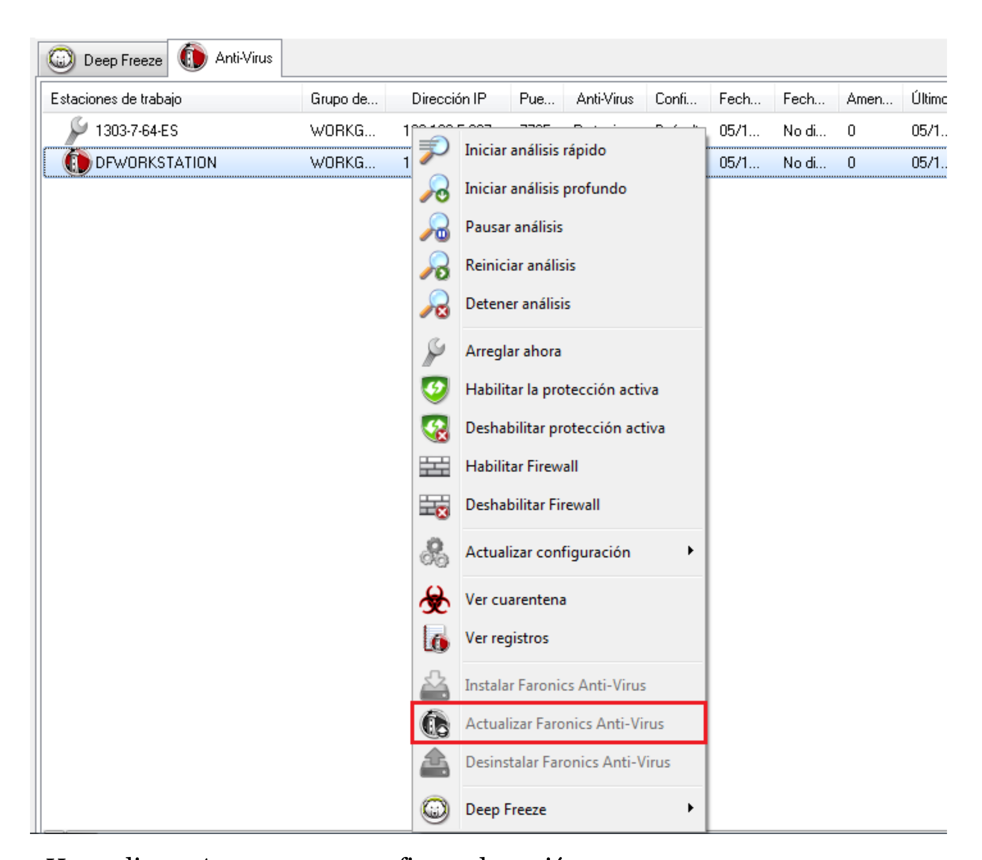
Si hay una nueva versión disponible, haga clic en *Descargar la última versión* para actualizar Faronics Anti-Virus.



Actualizar Faronics Anti-Virus

Si ha comprobado si hay actualizaciones disponibles y se ha encontrado una nueva versión, complete los siguientes pasos para actualizar a la nueva versión en la estación de trabajo:

1. Vaya a la ficha *Anti-Virus* en el panel *Estaciones de trabajo*.
2. Seleccione una estación de trabajo (o varias)
3. Haga clic con el botón secundario y seleccione *Actualizar Faronics Anti-Virus*.



4. Haga clic en *Aceptar* para confirmar la acción.

Se reiniciará la estación de trabajo y se actualizará el cliente de Faronics Anti-Virus en las estaciones de trabajo.



Desinstalar el cliente de Anti-Virus desde la consola Enterprise

Realice los siguientes pasos para desinstalar Faronics Anti-Virus en la estación de trabajo desde la consola Enterprise:

1. Vaya a la ficha *Anti-Virus* en el panel *Estaciones de trabajo*.
2. Seleccione una estación de trabajo (o varias)
3. Haga clic con el botón secundario y seleccione *Desinstalar Faronics Anti-Virus*.
4. Haga clic en *Aceptar* para confirmar la acción.

Se reiniciará la estación de trabajo y se desinstalará el cliente de Faronics Anti-Virus en las estaciones de trabajo.



Al desinstalar el cliente de Anti-Virus de la estación de trabajo, quedará la semilla de Deep Freeze.

La semilla de Deep Freeze no se puede desinstalar si el cliente de Anti-Virus está instalado en la estación de trabajo.



Deshabilitar Faronics Anti-Virus desde la consola Enterprise

Se puede deshabilitar Anti-Virus en la consola Deep Freeze si no es necesario usarlo.

Siga los pasos descritos a continuación para deshabilitar Faronics Anti-Virus desde la consola Deep Freeze:

1. Vaya a *Herramientas* > *Licencias* > *Licencia de Faronics Anti-Virus*.
2. Desactive la casilla de verificación *Deseo usar la consola Deep Freeze para administrar Faronics Anti-Virus*.



3. Haga clic en *Cerrar*.
4. Reinicie consola Enterprise para que la configuración surta efecto.





Control de la línea de comandos de Deep Freeze

En este capítulo se describe cómo utilizar los comandos de Deep Freeze.

Temas



Control de la línea de comandos de Deep Freeze (DFC.EXE)

El Control de la línea de comandos de Deep Freeze (DFC) ofrece a los administradores de red una mayor flexibilidad en la administración de los equipos Deep Freeze. DFC funciona en conjunto con herramientas de administración empresarial de terceros y/o soluciones de administración central. Esta combinación permite a los administradores actualizar los equipos rápidamente, según sea necesario.

Es importante destacar que DFC no es una aplicación autónoma. DFC se integra sin problemas con cualquier solución que pueda ejecutar archivos de secuencia de comandos, incluidas secuencias de comandos de inicio de sesión de una sola ejecución estándar.

Los comandos de DFC requieren una contraseña con derechos de la línea de comandos. No pueden utilizarse contraseñas de un solo uso.

Lista de todos los comandos al invocar DFC sin parámetros.

(32 bits) Los archivos se copian en
`<WINDOWS>\system32\DFC.exe`

(64 bits) Los archivos se copian en
`<WINDOWS>\syswow64\DFC.exe`

Valores de retorno de DFC

Al completar cualquier comando de DFC, DFC devuelve los siguientes valores:

Sintaxis	Descripción
`0`	SUCCESS o Boolean FALSE, para comandos que devuelven resultados booleanos
`1`	Boolean TRUE
`2 ERROR`	El usuario no tiene derechos de administrador
`3 ERROR`	El comando de DFC no es válido en esta instalación
`4 ERROR`	Comando no válido
`5 - * ERROR`	Error interno al ejecutar el comando



Control de la línea de comandos de Deep Freeze



Deep Freeze tiene un límite máximo de 63 caracteres para su contraseña. Si se introduce una contraseña con más caracteres, el comando no se ejecutará correctamente.

Sintaxis	Descripción
`Contraseña de DFC /BOOTTHAWED`	Reinicia el equipo en modo Descongelado; solo funciona en equipos en modo Congelado.
`Contraseña de DFC /THAWNEXTBOOT`	Configura el equipo para que se reinicie en modo Descongelado la próxima vez; solo funciona en equipos en modo Congelado y no fuerza el equipo a reiniciarse.
`Contraseña de DFC /BOOTFROZEN`	Reinicia el equipo en modo Congelado; solo funciona en equipos en modo Descongelado.
`Contraseña de DFC /FREEZENEXTBOOT`	Configura el equipo para que se reinicie en modo Congelado la próxima vez; solo funciona en equipos en modo Descongelado y no fuerza el equipo a reiniciarse.
`DFC get /ISFROZEN`	Consulta al equipo si está en modo Congelado. Devuelve el nivel de error 0 si está en modo Descongelado. Devuelve 1 si está en modo Congelado.
`DFC get /CLONE`	Establece el indicador de clonación para la creación de la imagen.
`Contraseña de DFC /CFG=[ruta] depfrz.rdx`	Sustituye la información de configuración de Deep Freeze. Funciona en equipos en modo Descongelado o Congelado. Los cambios en la contraseña se aplican de inmediato. Otros cambios requieren reinicio.
`DFC get /version`	Muestra el número de versión de Deep Freeze.
`Contraseña de DFC /UPDATE=[ruta de archivo de instalador]`	Configura el equipo para que se reinicie en modo Descongelado e instale una actualización de Deep Freeze.
`Contraseña de DFC /LOCK`	Deshabilita el teclado y el ratón en el equipo. Funciona en equipos en modo Congelado o Descongelado y no requiere un reinicio.
`Contraseña de DFC /UNLOCK`	Habilita el teclado y el ratón en el equipo. Funciona en equipos en modo Congelado o Descongelado y no requiere un reinicio.
`Contraseña de DFC /THAWLOCKNEXTBOOT`	Configura el equipo para que se reinicie en modo Descongelado con el teclado y el ratón deshabilitados; solo funciona en equipos en modo Congelado.



Sintaxis	Descripción
`Contraseña de DFC /BOOTTHAWEDNOINPUT`	Reinicia el equipo en modo Descongelado con el teclado y el ratón deshabilitados; solo funciona en equipos en modo Congelado.
`DFC get /LICENSESTATUS`	Muestra el estado de la licencia y la fecha de caducidad de la licencia (si procede). Los diferentes tipos posibles de licencia y los códigos de retorno asociados son: 111: Sin licencia, Deep Freeze no tiene licencia y funcionará en modo *Evaluación* durante 30 días después de la instalación. 112: Evaluación, tiene licencia para una evaluación con fecha de caducidad fija. 113: Con licencia, tiene licencia sin fecha de caducidad. 114: Caducado, el periodo de evaluación ha caducado.
`DFC get /LICENSETYPE`	Muestra el estado de la licencia y la fecha de caducidad de la licencia (si procede). Los diferentes tipos posibles de licencia y los códigos de retorno asociados son: 111: Ninguna (sin licencia): Deep Freeze no tiene licencia y funcionará en modo *Evaluación* durante 30 días después de la instalación. 112: Evaluación, tiene licencia para una evaluación con fecha de caducidad fija. 113: Estándar (con licencia), tiene licencia sin fecha de caducidad. 114: Prohibida la reventa, tiene licencia sin fecha de caducidad.
`Contraseña de DFC /LICENSE=clavedelicencia`	Cambia la clave de licencia. *contraseña* es la contraseña del administrador de Deep Freeze. *clavedelicencia* es la clave de licencia de Deep Freeze. Si hay un error, se mostrarán los siguientes códigos de error: 101: la clave de licencia no es válida 102: la clave de licencia proporcionada ha caducado.



Sintaxis	Descripción
`Contraseña de DFC /WU [/UNLOCK] [/NOMSG | /NOMESSAGE] [/THAW]`	Se descargarán las actualizaciones de Windows y se instalarán en la estación de trabajo. [/UNLOCK] Parámetro opcional para habilitar el teclado y el ratón durante la actualización de Windows. [/NOMSG | /NOMESSAGE] Parámetro opcional para omitir todos los mensajes informativos o de advertencia de Deep Freeze durante la actualización de Windows. [/THAW] Parámetro opcional para volver a poner el equipo en modo Descongelado una vez finalizada la actualización de Windows.
`DFC password /ENDTASK`	Finaliza la tarea de estación de trabajo en curso y reinicia el equipo en modo Congelado. Las tareas de archivo por lotes y las tareas de periodo de descongelación finalizarán inmediatamente. Las tareas de actualización de Windows se completarán.



Sintaxis de la línea de comando de Faronics Anti-Virus

Siga los pasos descritos a continuación para ejecutar los comandos de Faronics Anti-Virus:

1. En la estación de trabajo, vaya a *<Directorio del sistema>:\Archivos de programa\Faronics\Faronics Anti-Virus Enterprise* desde el símbolo del sistema.
2. Introduzca `AVECLI/[Comando]`

Estos son los comandos disponibles:

Sintaxis	Descripción
`definitionversion`	Muestra la versión de las definiciones de virus.
`scanengineversion`	Muestra la versión del motor de análisis.
`updatedefs`	Actualiza y aplica las definiciones de virus.
`fixnow`	Descarga las últimas definiciones de virus. Habilita la protección activa y la protección de correo electrónico. Realiza el análisis a fondo predeterminado
`scanquick`	Inicia un análisis rápido.
`scandeep`	Inicia un análisis a fondo.
`enableap`	Habilita la protección activa.
`applydefs [ruta de las definiciones]`	Aplica el archivo de definiciones desde una ubicación guardada.
`fixnow /quick`	Realiza un *análisis rápido* si es aplicable.
`resetpolicy`	Restablece la directiva predeterminada de Anti-Virus.
`setlicense[clave]`	Aplica una clave de licencia determinada.

Sintaxis:

```
AVECLI/definitionversion
```



Apéndice A Puertos y protocolos

La clave para configurar la arquitectura de Deep Freeze es conocer qué puertos utilizar. Lo importante es saber qué puertos se están utilizando en la red y usar puertos que no entren en conflicto con los utilizados. El puerto predeterminado (7725) se ha registrado oficialmente para Deep Freeze.

Estos son los tres elementos que conforman la arquitectura de Deep Freeze:

- Cliente (con semilla instalada)
- Consola remota (servicio local habilitado)
- Consola (se conecta a la consola remota)

Siempre que los clientes y la conexión de la consola remota utilicen el mismo puerto, no debería haber ningún conflicto entre los distintos componentes:



Los puertos también pueden utilizarse para dividir los clientes. Si el servicio local está configurado para funcionar con tres puertos (7725, 7724 y 7723), las consolas Enterprise pueden conectarse con los tres puertos para visualizar un conjunto de clientes distintos en cada puerto.

En el diagrama anterior, los clientes utilizan los protocolos TCP y UDP para comunicarse con la consola remota. Las consolas que se conectan con la consola remota solo utilizan el protocolo TCP para comunicarse con la consola remota. Es importante recordar los puertos y protocolos que se utilizan para evitar que los firewall, conmutadores o enrutadores los bloqueen.





Apéndice B Ejemplos de redes

Los siguientes ejemplos muestran distintos casos relacionados con el servicio local o la consola remota.

- Ejemplo 1: subred simple
- Ejemplo 2: varias subredes, un servicio local
- Ejemplo 3: varios puertos, acceso remoto a consola
- Ejemplo 4: varias subredes, varios servicios locales

Cada ejemplo explica la manera en que los componentes de Deep Freeze interactúan en distintos entornos de red.



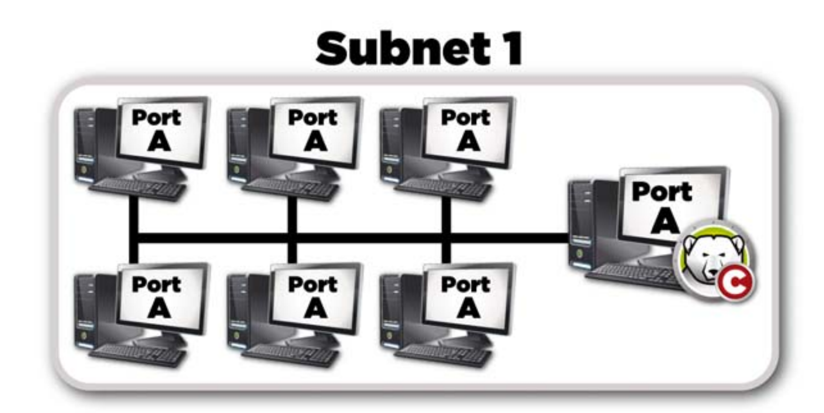
En los siguientes ejemplos, los equipos cliente tienen la instalación de estación de trabajo de Deep Freeze o la semilla de estación de trabajo instaladas. Ambas instalaciones contienen el componente de comunicación que entabla diálogo con la consola o la consola remota. La diferencia entre la instalación de estación de trabajo y la semilla de estación de trabajo es que la instalación de estación de trabajo instala Deep Freeze, mientras que la semilla solo contiene el componente de comunicación.



Ejemplo 1: subred simple

En este entorno, todos los equipos cliente están incluidos en la misma subred que el equipo de la consola. Este entorno no requiere una consola remota, aunque podría usarse una. En este ejemplo, no se utiliza la consola remota. Este es el entorno de red más simple. También es el más fácil de configurar.

El siguiente diagrama muestra la topología de la red:

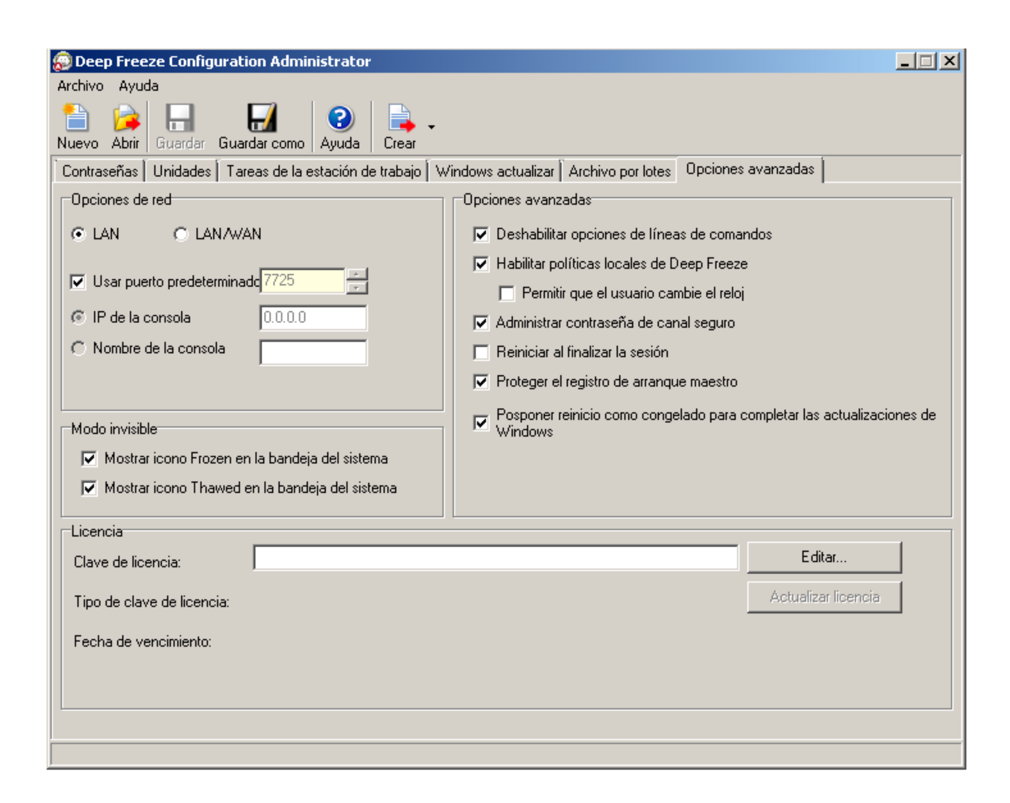


Los equipos cliente, representados por los iconos con forma de equipo, están situados en la misma subred que el equipo de la consola Deep Freeze Enterprise, representado por el icono de la consola Deep Freeze.

En este caso, los clientes utilizan el puerto A, mientras que la consola ha configurado una conexión de servicio local para el mismo puerto. Este puerto se configura en la ficha *Opciones avanzadas* antes de crear el archivo de instalación de estación de trabajo o la semilla de estación de trabajo.



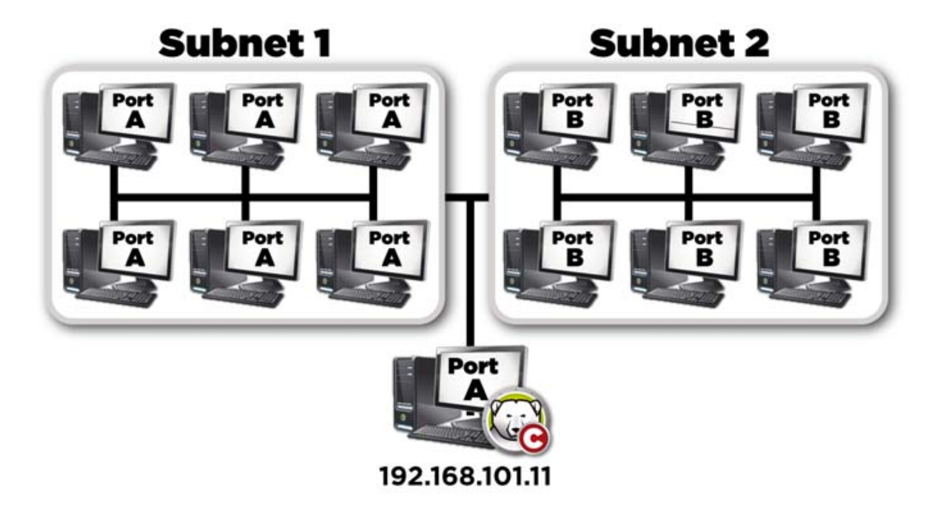



Deep Freeze Configuration Administrator
Archivo Ayuda
Nuevo
Abrir
Guardar
Guardar como
Ayuda
Crear
Contraseñas
Unidades
Tareas de la estación de trabajo
Windows actualizar
Archivo por lotes
Opciones avanzadas
Opciones de red
LAN
LAN/WAN
Usar puerto predeterminado
7725
IP de la consola
0.0.0.0
Nombre de la consola
Modo invisible
Mostrar icono Frozen en la bandeja del sistema
Mostrar icono Thawed en la bandeja del sistema
Opciones avanzadas
Deshabilitar opciones de líneas de comandos
Habilitar políticas locales de Deep Freeze
Permitir que el usuario cambie el reloj
Administrar contraseña de canal seguro
Reiniciar al finalizar la sesión
Proteger el registro de arranque maestro
Posponer reinicio como congelado para completar las actualizaciones de Windows
Licencia
Clave de licencia:
Editar...
Tipo de clave de licencia:
Actualizar licencia
Fecha de vencimiento:



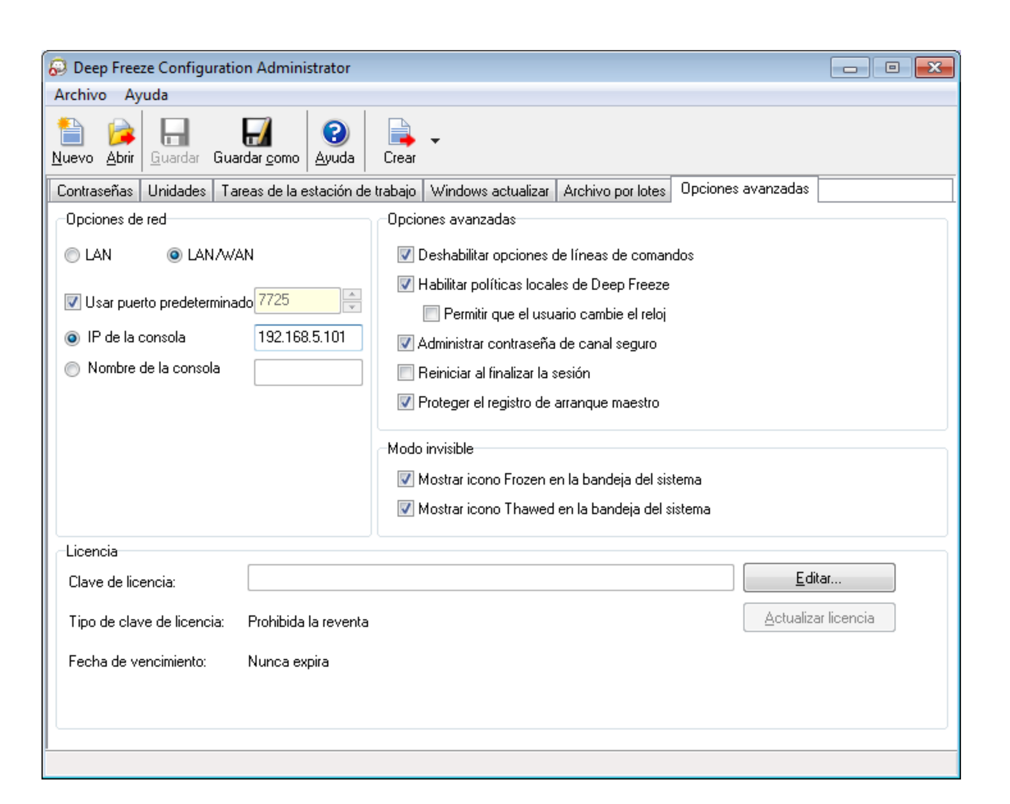
Ejemplo 2: varias subredes, un servicio local

En este entorno, los clientes están ubicados en más de una subred. Aun así, se utiliza solo una consola. Este entorno no requiere una consola remota, aunque podría usarse una. El siguiente diagrama muestra la topología de la red:



En este escenario (similar a *Ejemplo 1: subred simple*), ambos clientes y la conexión alojada por la consola utilizan el mismo puerto. Este puerto se configura en el Administrador de configuración de Deep Freeze en la ficha *Opciones avanzadas* antes de crear el archivo de instalación de estación de trabajo o la semilla de estación de trabajo.

Para que los clientes estén visibles, es preciso configurarlos para que utilicen una conexión LAN/WAN. Al seleccionar la opción LAN/WAN, aparece un campo de *IP de la consola*. Especifique la IP del equipo que ejecutará la consola Enterprise. La ficha *Opciones avanzadas* que aparece a continuación muestra un ejemplo de estos ajustes:

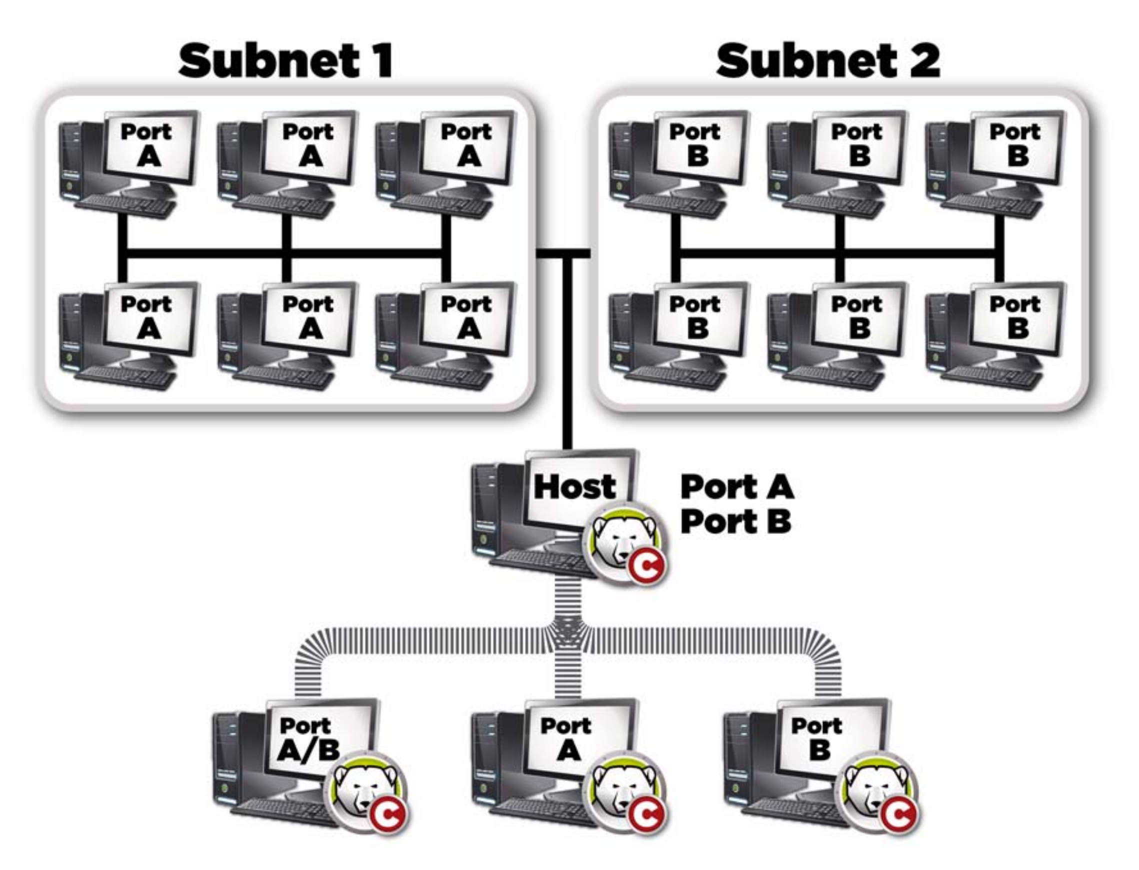


Deep Freeze Configuration Administrator
Archivo
Ayuda
Nuevo
Abrir
Guardar
Guardar como
Ayuda
Crear
Contraseñas
Unidades
Tareas de la estación de trabajo
Windows actualizar
Archivo por lotes
Opciones avanzadas
Opciones de red
LAN
LAN/WAN
Usar puerto predeterminado
7725
IP de la consola
192.168.5.101
Nombre de la consola
Opciones avanzadas
Deshabilitar opciones de líneas de comandos
Habilitar políticas locales de Deep Freeze
Permitir que el usuario cambie el reloj
Administrar contraseña de canal seguro
Reiniciar al finalizar la sesión
Proteger el registro de arranque maestro
Modo invisible
Mostrar icono Frozen en la bandeja del sistema
Mostrar icono Thawed en la bandeja del sistema
Licencia
Clave de licencia:
Editar...
Tipo de clave de licencia:
Prohibida la reventa
Actualizar licencia
Fecha de vencimiento:
Nunca expira



Ejemplo 3: varios puertos, acceso remoto a consola

En este entorno, los clientes se ubican nuevamente en varios puertos. En este caso, se utiliza más de una consola. Se accede a varias consolas mediante un servicio local cuyo administrador (host) ha dado a conocer la información de la conexión. El siguiente diagrama muestra la topología de la red:



En este caso, el host ha configurado una conexión utilizando el servicio local. El diagrama anterior muestra otras tres consolas que se conectan al host para visualizar los clientes en función de sus puertos. Las consolas no tienen que formar parte de subredes individuales siempre y cuando puedan ver el host.

Más específicamente, la consola conectada a través del puerto A/B puede visualizar la consola host, así como cada uno de los equipos individuales asignados a los puertos A y B. Las otras consolas conectadas a través del puerto B pueden visualizar el host y solamente los equipos asignados al puerto B.



Ejemplo 4: varias subredes, varios servicios locales

En este ejemplo, hay dos ubicaciones separadas.

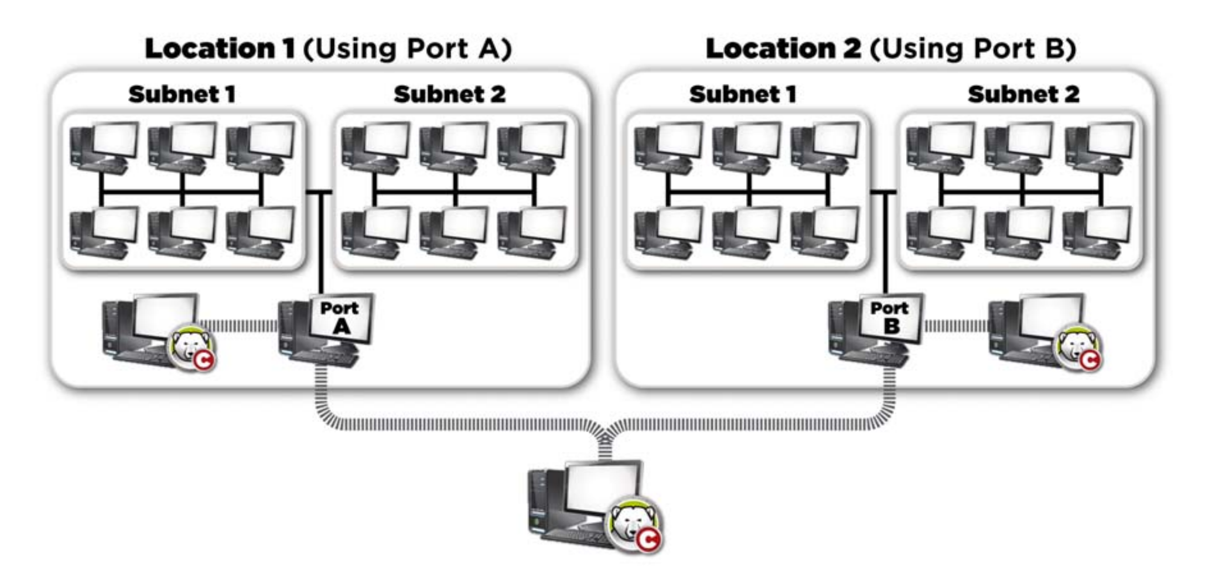
A continuación, se muestra una lista de consideraciones acerca de este ejemplo en particular:

- las ubicaciones se separan y solo tienen un mínimo de conexión entre sí
- cada ubicación tiene un administrador de red que es responsable de proteger a Deep Freeze en esa ubicación
- ambas ubicaciones necesitan ser administradas por una tercera ubicación

En este ejemplo, las consolas remotas se configuran en cada ubicación y se utiliza un servicio local:

- La Ubicación 1 (una sala de informática de un campus) utiliza el puerto A para comunicarse con los clientes y las conexiones alojadas por la consola. Los equipos de la biblioteca de la escuela utilizan el puerto B. La consola del departamento de soporte técnico utiliza las conexiones alojadas por las consolas de la sala de informática y las de la biblioteca.
- Toda consola que no se comunica directamente con un equipo debe tener el servicio local desactivado.

El siguiente diagrama muestra la topología de la red:



El beneficio de esta configuración es que permite que todos los paquetes enviados desde los clientes en la Ubicación 1 estén incluidos en esa ubicación. Cuanto menor sea la distancia que deba recorrer un paquete, mayor será la posibilidad de que llegue.

El administrador de la sala de informática puede conectarse al servicio local en la misma ubicación 1, pero no puede conectarse con el servicio local de la biblioteca. Esto se debe a que el administrador de la sala de informática no conoce la contraseña para acceder al servicio local de la biblioteca. Lo mismo ocurre con el administrador de la biblioteca. Si el soporte técnico conoce la contraseña de los dos servicios locales (sala de informática y biblioteca), ambas ubicaciones pueden conectarse al servicio local con el fin de administrar todos los clientes.





Apéndice C Solucionar un problema de conexión con la consola remota

No hay clientes en la consola

Estas son algunas de las razones comunes por las que los clientes no aparecen en la consola.

1. La consola y los clientes no tienen la configuración de red correcta.

Si la consola está configurada para ejecutarse con un puerto y los clientes utilizan otro, no podrán verse entre sí. Asimismo, si los equipos se configuran para LAN/WAN, la IP debe ser igual que la IP del equipo donde se está ejecutando la consola.

La configuración LAN predeterminada funciona siempre y cuando todos los equipos que ejecutan el equipo y la consola se encuentren en la misma subred. Sin embargo, si se está ejecutando una VLAN o si hay varias subredes donde están los clientes, la instalación del equipo debe configurarse para que se ejecute con la configuración de LAN/WAN.

2. Hay algo en la red que bloquea el puerto utilizado entre la consola y los clientes.

Compruebe que haya conexión haciendo ping. Los clientes no pueden enviar paquetes a la consola/consola remota porque no parece haber una ruta hasta el host. Los intentos de hacer ping en la IP de la consola/consola remota no parecen funcionar. Para resolver este problema, asegúrese de que los dos equipos puedan conectarse entre sí.

Si un servidor, un enrutador o un conmutador de la red no permiten que el puerto se conecte, los clientes no podrán visualizarse. El puerto predeterminado que se utiliza es 7725.

3. Las estaciones de trabajo fueron creadas con un código de personalización distinto del de la consola.

La primera vez que se ejecuta el Administrador de configuración de Deep Freeze, se pedirá que se introduzca un código de personalización. Este código es muy importante porque cifra el software. Esto significa que todas las estaciones de trabajo creadas se cifrarán con este código de personalización. Si la consola se creó utilizando otro administrador que fue instalado con un código de personalización distinto, esta no podrá ver las estaciones de trabajo creadas con el código original. Las estaciones de trabajo y la consola deben crearse con un Administrador de configuración instalado con el mismo código de personalización.



El puerto está en Error de uso al iniciar la consola

Al intentar iniciar la consola, aparece el mensaje de error *No se puede iniciar la consola: el puerto está en uso*. Hay varias razones por las cuales puede aparecer este mensaje de error:

1. Hay una instalación de estación de trabajo/semilla de estación de trabajo de Deep Freeze instalada con el mismo puerto que la consola o en el mismo equipo.

Es posible que Deep Freeze haya sido instalado en modo invisible (el icono no aparece en la bandeja del sistema). La semilla no muestra un icono. La mejor prueba es ejecutar un archivo de instalación de estación de trabajo en el equipo. Si se muestra la opción de desinstalación, el archivo de instalación de estación de trabajo o la semilla de estación de trabajo están instalados y pueden desinstalarse. Si la opción de desinstalar no aparece, el archivo de instalación de estación de trabajo o la semilla de estación de trabajo no están instalados.

La solución más simple sería primero desconectar el servicio local y después conectarse a una consola a la que puede accederse de forma remota.

2. Otro programa o servicio está utilizando el puerto en este equipo.

Esto puede incluir la ejecución de un rastreador de puertos en el equipo en cuestión para ver los puertos que están abiertos. Existen varias herramientas disponibles en Internet para ejecutar esta acción. La aplicación *netstat.exe* disponible en Windows también debe mostrar si el puerto que está utilizando Deep Freeze ya está en uso.

3. El cable de red está desconectado.

Este mensaje puede aparecer si no hay ninguna conexión de red en el equipo.

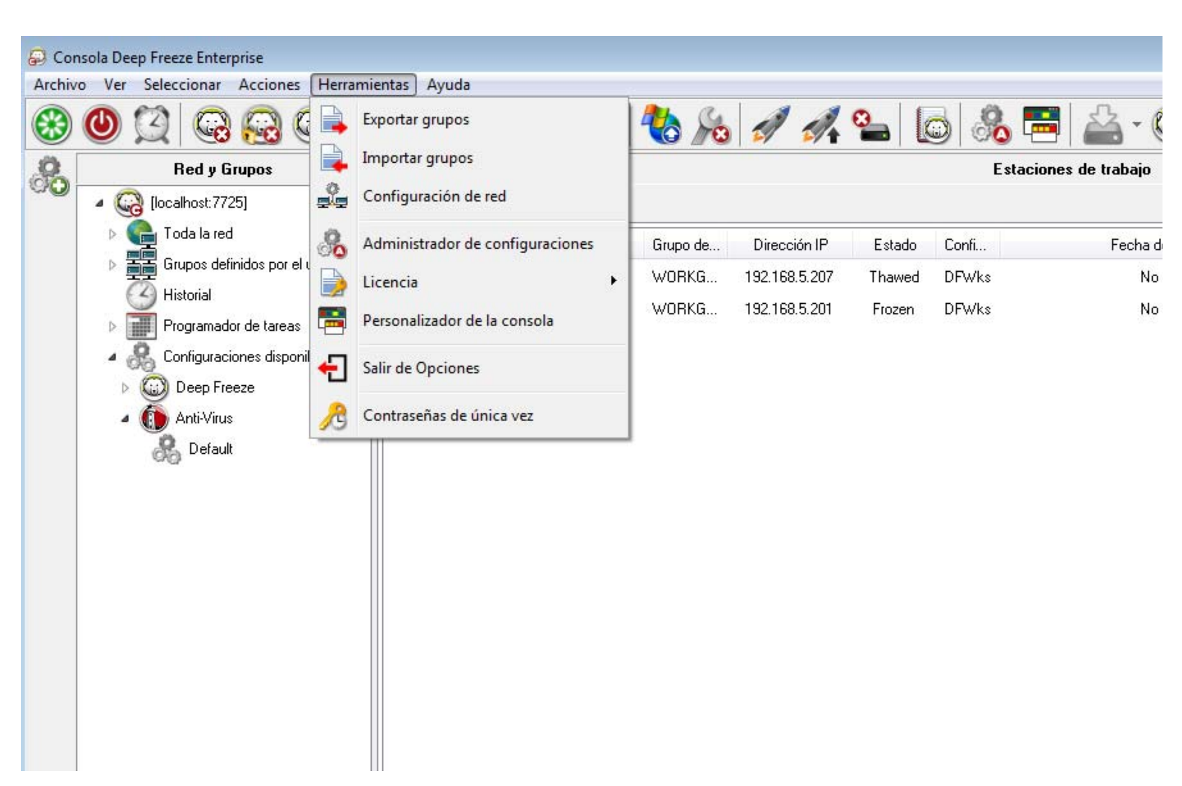


Apéndice D Creación de una consola Deep Freeze Enterprise personalizada

La consola Deep Freeze Enterprise permite crear una nueva consola Enterprise con capacidades limitadas. Una consola personalizada y limitada puede distribuirse en su organización para permitir a ciertos usuarios realizar tareas deseadas sin que tengan acceso a todas las capacidades de la consola Enterprise.

En este ejemplo, crearemos una consola limitada para distribuir a un profesor o instructor de una sala de informática. En este caso, queremos que el profesor pueda reiniciar los equipos, bloquear el teclado y el ratón según lo desee y enviar mensajes a los estudiantes. Sin embargo, no queremos que el profesor pueda reiniciar los equipos en modo Descongelado, desinstalar Deep Freeze ni realizar otras tareas exclusivas del departamento de TI.

Para iniciar el Personalizador de la consola, vaya a *Herramientas* > *Personalizador de la consola*.



Dejaremos *Funciones de la consola* > *Activación* seleccionado. Esto garantiza que si la nueva consola se traslada a un equipo diferente, será preciso introducir la contraseña de un solo uso en el equipo al que se ha trasladado la nueva consola. Si esta precaución de seguridad no es una preocupación en su entorno, no seleccione esta opción.

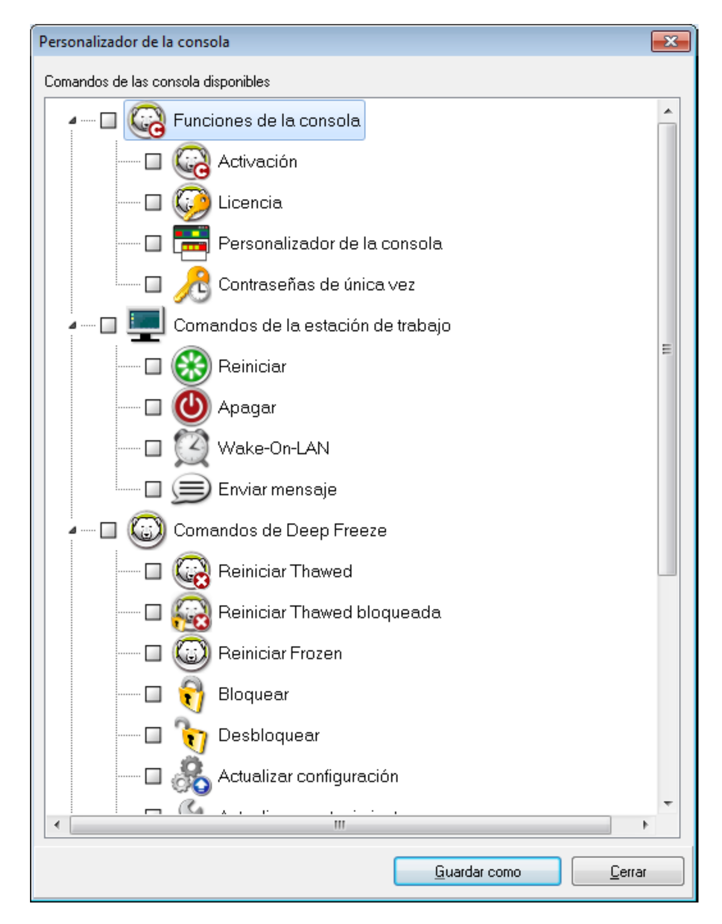
Funciones de la consola> *Contraseña de un solo uso* no está seleccionada porque no queremos que un profesor pueda reiniciar el equipo en modo Descongelado bajo ninguna circunstancia. Si un profesor reinicia el equipo en modo Descongelado, los estudiantes podrían instalar software innecesario en el equipo que será retenido incluso después de reiniciarlo.

Dejaremos todas las opciones de *Comandos de estación de trabajo* seleccionadas porque queremos que los profesores puedan enviar mensajes a estudiantes y que puedan apagar, reiniciar y activar los equipos según lo requieran.



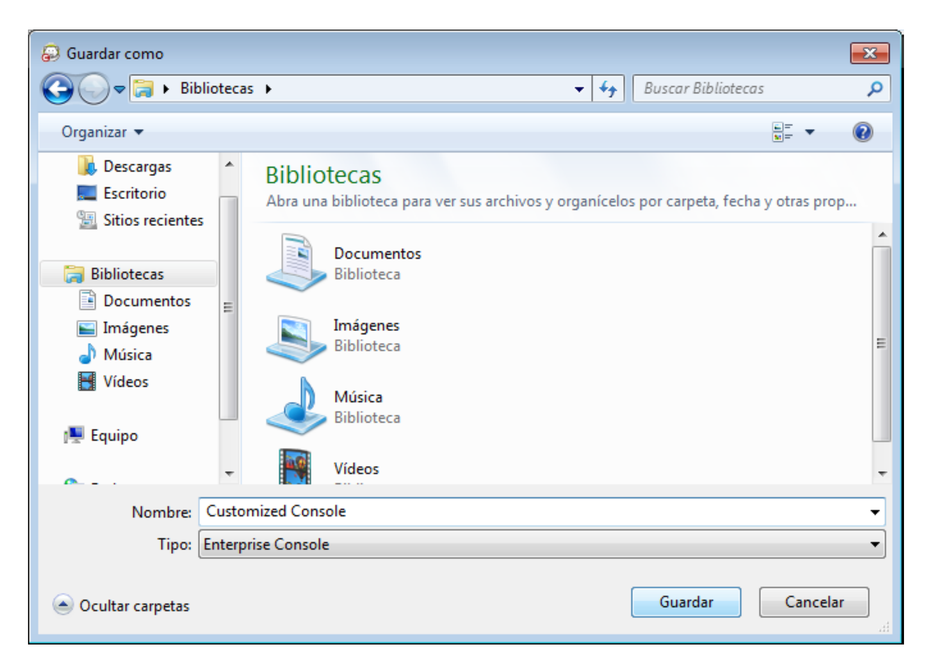
Solo dejaremos tres opciones seleccionadas en Comandos de Deep Freeze: *Desbloquear*, *Bloquear* y *Reiniciar como Congelado*. Esto permitirá a los profesores bloquear (y desbloquear) el teclado y el ratón en los equipos de los estudiantes, así como reiniciar los equipos en modo *Congelado* (por si alguna vez el personal de TI se deja un equipo en modo *Descongelado* por accidente). Dejar todas las otras opciones deseleccionadas garantizará que los profesores no puedan modificar el equipo de forma permanente.

Por último, desactivaremos todos los *Comandos de instalación/desinstalación de estación de trabajo* y todos los *Comandos del Programador* porque no queremos que nuestro profesor use ninguna de estas opciones.



Una vez se hayan seleccionado todas las opciones, haga clic en *Guardar como* para guardar una nueva consola Enterprise. Se mostrará un cuadro de diálogo *Guardar como* estándar:





Guarde la nueva consola Enterprise limitada y distribúyala a los usuarios requeridos.





Apéndice E Archivos de acción de Deep Freeze: ejemplo de RDC

Archivos de acción de Deep Freeze

Un archivo de acción de Deep Freeze es un archivo XML que permite a los administradores definir funciones adicionales en la consola Deep Freeze Enterprise. Un archivo de acción define un método para invocar un archivo por lotes externo y transmitir algo de información (por ejemplo, la dirección IP de la máquina, nombres de equipos) a una secuencia de comandos o archivo por lotes.

Los archivos de acción simplemente invocan programas o secuencias de comandos externos. Por ello, puede usarse cualquier lenguaje de secuencia de comandos que pueda invocarse desde la línea de comandos.

Ejemplo de archivo de acción

La estructura para el archivo de acción de Deep Freeze que usaremos se muestra más abajo. El archivo *DFEntConsoleCustomActions.xml* está disponible en *C:\Archivos de programa\Faronics\Deep Freeze 7 Enterprise*. El archivo puede editarse para agregar acciones adicionales como la que se explica más abajo:

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Archivo de acción personalizado predeterminado de Deep Freeze-->
<CUSTOMDEFINEDACTIONS>
 <ACTION1>
  <CAPTION>
   <ENGLISH>Control with RDC</ENGLISH>
   <GERMAN>Control with RDC German</GERMAN>
   <JAPANESE>Control with RDC Japanese</JAPANESE>
   <SPANISH>Control with RDC Spanish</SPANISH>
   <FRENCH>Control with RDC French</FRENCH>
   <CHINESE>Control with RDC Chinese</CHINESE>
</CAPTION>
  <FILEMENU>Y</FILEMENU>
  <POPUPMENU>Y</POPUPMENU>
  <SILENT>Y</SILENT>
  <SUBITEMS/>
  <PARAMS/>
  <SYNC/>
  <LOG/>
  <EXECUTE>C:\Windows\system32\mstsc.exe /v:%%WKSNAME%% /f</EXECUTE>
  <WORKDIR>C:\Windows\system32\</WORKDIR>
```

En el ejemplo que se muestra arriba, el archivo de acción personalizado contiene el comando para ejecutar el Escritorio remoto en el equipo de la consola y conectar el equipo remoto especificado en el parámetro `%%WKSNAME%%`.

El archivo *DFEntConsoleCustomActions.xml* contiene 3 muestras:

- Control con RDC
- Ejecución remota
- Enviar e instalar archivo MSI



Para obtener información acerca de cómo utilizar estas muestras, consulte la sección *Configuración de acciones personalizadas*. Puede editar el archivo *DFEntConsoleCustomActions.xml* según sus necesidades.



Estructura del archivo de acción de Deep Freeze

El siguiente esquema XML describe las acciones personalizadas definidas disponibles para el usuario. Pueden guardarse varios archivos XML según la cantidad de comandos requeridos. Cada archivo debe guardarse en la carpeta de la consola y el atributo "solo lectura" no debe estar seleccionado.

Cualquier cambio realizado debe ir acompañado de un reinicio de la consola Deep Freeze para que surta efecto.

Parámetro	Uso
<?xml version=”1.0” encoding=”UTF-8”?>	
<CUSTOMDEFINEDACTIONS>	
<CAPTION>	El texto que aparece en el menú o submenú del archivo
<ENGLISH>Caption</ENGLISH>	Texto en diferentes idiomas
<GERMAN>Caption</GERMAN>	Texto en diferentes idiomas
<JAPANESE>Caption</JAPANESE>	Texto en diferentes idiomas
<SPANISH>Caption</SPANISH>	Texto en diferentes idiomas
<FRENCH>Caption</FRENCH>	Texto en diferentes idiomas
<CHINESE>Caption</CHINESE>	Texto en diferentes idiomas
<FILEMENU>y</FILEMENU>	Define si esta sección estará en el menú del archivo
<POPUPMENU>y</POPUPMENU>	Define si esta sección estará en el menú emergente que aparece al hacer clic con el botón secundario
<SILENT>y</SILENT>	Define si se pedirá al usuario un mensaje de confirmación
<SUBITEMS>	En subelementos, puede definirse el elemento que depende de este elemento
</SUBITEMS>	Si se definen los subelementos, entonces se ignorará la acción para estos elementos
<SYNC>y</SYNC>	Especifica si el comando se ejecutará de forma sincronizada o asíncrona
<PARAMS>	Al elegir esta acción, se pedirá al usuario que introduzca parámetros personalizados
<PASSWORD>	Nombre en el parámetro
<VAR>%PARAM1%</VAR>	Nombre de la variable que se utilizará en EXECUTE
<ENGLISH>USERNAME Param (ENGLISH)</ENGLISH>	Texto en diferentes idiomas



Parámetro	Uso
<GERMAN>USERNAME Param (GERMAN)</GERMAN>	Texto en diferentes idiomas
<JAPANESE>USERNAME Param (JAPANESE)</JAPANESE>	Texto en diferentes idiomas
<SPANISH>USERNAME Param (SPANISH)</SPANISH>	Texto en diferentes idiomas
<FRENCH>USERNAME Param (FRENCH)</FRENCH>	Texto en diferentes idiomas
<CHINESE>USERNAME Param (CHINESE)</CHINESE>	Texto en diferentes idiomas
</CAPTION>	
</USERNAME>	
</PARAMS>	
<LOG>	Define el comportamiento del archivo de registro
<APPEND>y</APPEND>	Define si se anexará el archivo de registro o si se creará uno nuevo
<FILENAME>c:\a1command.log</FILENAME>	Define el nombre del archivo
<EXECUTE>c:\windows\vpn.exe %%IP%% %USERNAME% %PASSWORD% %%WKSNAME%%</EXECUTE>	Define el comando que se ejecutará Aquí pueden usarse parámetros y/o elementos de la consola
<WORKDIR>c:\windows</WORKDIR>	Define el directorio de trabajo



Parámetros de la consola

Los siguientes parámetros de la consola pueden pasarse a la aplicación o secuencia de comandos ejecutada a través de la consola Enterprise:

Parámetro	Uso
%%WKSNAME%%	Nombre de la estación de trabajo
%%DOMAIN%%	Dominio de la estación de trabajo
%%IP%%	IP de la estación de trabajo
%%PORT%%	Puerto de la estación de trabajo
%%STATUS%%	Estado de la estación de trabajo
%%CFGDATETIME%%	Configuración de fecha/hora de la estación de trabajo
%%MAC%%	Dirección MAC de la estación de trabajo
%%DFVERSION%%	Versión de Deep Freeze de la estación de trabajo

